مراقبة الانترنت

و أثرها على الحريّات العامة

الدكتور

بشيخ محمد حسين



مراقبة الانترنت و أثرها على الحريّات العامة

د. بشيخ محمد حسين

الناشر

المكتب العربي للمعارف

عنوان الكتاب: مراقبة الإنترنت وأثرها على الحريات العامة
اسم المؤلف: د. بشيخ محمد حسين
تصميم الغلاف: عمرو حمدي
24x17 سم.
رقم الإيداع: 2018/ 9282
الترقيم الدولي: 978-977 812-280-0

الناشر

المكتب العربي للمعارف



26 شارع حسين خضر من شارع عبدالعزيز فهمي
ميدان هليوبوليس - مصر الجديدة - القاهرة



02-264231100
01283322273



malghaly@yahoo.com
elmaktb.elarabe.llmaref



www.mam-books.com



2019م

بسم الله الرحمن الرحيم

يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ

[الحجرات: 12.]

عن أبي هريرة –رضي الله عنه– قال: قال رسول الله –صلى الله عليه وسلم :إياكم والظن، فإن الظن أكذب الحديث، ولا تحسسوا ولا تجسسوا ولا تنافسوا ولا تحاسدوا ولا تباغضوا، ولا تدابروا وكونوا عباد الله إخواناً.

رواه البخاري (6064)، ومسلم (2563).

" إن المراقبة تخطت الممارسة التقليدية في التنصت على اتصالات شخص يُشتبه في ضلوعه في أنشطة مريبة ورصد تحركاته، وأصبحت اليوم تغطي الاتصالات الهاتفية، والبريد الالكتروني، والرسائل النصية، وتاريخ عمليات البحث التي تُجريها على الانترنت، وما تشتريه، ومن هم أصدقاؤك، وأين تتردد، ومن تحب ".

إدوارد سنودن

الموظف السابق في

وكالة الأمن القومي الاميركية.

إهـــداء

أهدي أولى ثماري إلى من حملتني وهنا على وهن إلى من غمرتني بحبها وعطفها و حنانها إلى التي سهرت الليالي كي أنام وتعبت كي أرتاح التي رعتني صغيرا وحملت همي كبيرا ، إلى رمز الحنان والمحبة... فإليك أمي ثم إليك أمي ثم إليك يا أماه الرائعة

إلى من أنار لي مشوار حياتي ، إلى من كان دعما لي في دراستي إلى من منحني كل شيئ

ولم ينتظر مني أي شيئ...

إلى العزيز الغالي إليك يا أبتي الرائع

أطال الله في عمركما و حفظكما من كل سوء

بكل الحب... إلى رفيقة دربي إلى من سارت معي نحو الحلم.. خطوة بخطوة بذرناه معاً.. وحصدناه معاً

وسنبقى معاً.. بإذن الله... جزاك الله خيراً

إلى أبنائي... القمرين عماد حسن وحسين إياد... النور الذي يضيئ عمري

إلى من حبهم يجرى فى عروقى ويلهج بذكراهم فؤادى الى اخوانى و أخواتي.

إلى كل زملائي وزميلاتي.

إلى كل من أضاء لي شمعة في طريق العلم أو ذلل لي كل عقبة في طريق النجاح

أهدي هذا العمل المتواضع

قائمة أهم المختصرات

المختصرات باللغة الفرنسية:

:LISTE DES PRINCIPALES ABRÉVIATIONS

Aff. : Affaire
Al. : Alinéa
Art. : Article
C/ : Contre
CA : Cour d'appel
Cah. Cons. Const. : Les Cahiers du Conseil constitutionnel
Cass. : Cour de cassation
CE : Conseil d'Etat
CEDH : Cour européenne des Droits de l'Homme
Ch. : Chambre
Chap. : Chapitre
Chron. : Chronique
CIDH : Cour Interaméricaine des Droits de l'Homme
Circ. : Circulaire
Civ. : Chambre civile de la Cour de cassation
CNIL : Commission Nationale Informatique et Libertés
Coll. : Collection
Comm. : Commentaire
Cons. : Considérant
Cons. Const. : Conseil constitutionnel

Cons. E. : Conseil de l'Europe
Conv. EDH : Convention européenne des Droits de l'Homme
CPC : Code de procédure civile
CPCE : Code des postes et communications électroniques
C. pén. : Code penal
CPI : Code de la propriété intellectuelle
CPP : Code de procédure pénale
Crim. : Chambre criminelle de la Cour de cassation
D. : Recueil Dalloz
DDHC : Déclaration des Droits de l'Homme et du Citoyen
Déc. : Décision
Décl. : Déclaration
Délib. : Délibération
Dir. : Directive communautaire
Doc. : Document
Doc. fr. : Documentation française
Doct. : Doctrine
Dr. : Pén. Revue Droit pénal
D. doc. : Dalloz droit social
DUDH : Déclaration Universelle des Droits de l'Homme
Ed. : Edition
Eds. : Editeurs
FAI : Fournisseur d'accès à Internet
Fasc. : Fascicule
G29 : Groupe de l'Article 29
Gaz. Pal. : Gazette du Palais

HADOPI : Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet.

JCP A : Revue La Semaine Juridique, édition administrations et collectivités territoriales

JO : Journal Officiel

JOCE : Journal Officiel des Communautés Européennes

JOUE : Journal Officiel de l'Union Européenne (à partir de 2003)

LCEN : Loi sur la confiance dans l'économie numérique

Lég. : Légipresse

LGDJ : Librairie Générale du Droit et de Jurisprudence

LIL : Loi Informatique et Libertés

LPA : Les Petites Affiches

Obs. : Observations

OCDE : Organisation de Coopération et de Développement Economiques

ONU : Organisation des Nations Unies

Op. cit. : Opus citatum: « oeuvre citée »

Ord. : Ordonnance

Ord. réf. : Ordonnance de référé

OSCE : Organisation pour la Sécurité et la Coopération en Europe

P. : Page

P2P : « Peer to peer », pair à pair

P. ex. : Par exemple

Préc. : Précité

Propr. Industr : Revue Propriété Industrielle
PUF : Presses Universitaires de France
QPC : Question Prioritaire de Constitutionnalité
Rapp. : Rapport
Rec. : Recommandation
Règl. : Règlement
Rép. : Répertoire
Req. : Requête
Rés. : Résolution
Rev. Sc. Crim. : Revue des Sciences Criminelles
RLDA : Revue Lamy Droit des Affaires
RLDI : Revue Lamy Droit de l'Immatériel
S. : Suivants
S. dir. : Sous direction
Sect. : Section
SI : Système d'Information STAD
: Système de Traitement Automatisé des Données
TA : Tribunal Administratif
T. corr. : Tribunal correctionnel
TGI : Tribunal de grande instance
TIC : Technologies d'Information et de Communication
Trad. : Traduction

UIT : Union Internationale des Télécommunications

UNESCO : Organisation des Nations unies pour l'éducation, la science et la culture
V. : Voir
Vol. : Volume

مقدمة

إن تأثير تكنولوجيات المعلومات والاتصال أساسي على الحريات العامة، ولا سيما فيما يتعلق بحرية التعبير وحماية حرمة الحياة الخاصة. وتشهد هذه الحريات العامة بعدا جديدا عندما يصبح من الممكن باستخدام المعلومات الرقمية خلق صور للفرد – "الشخصية الإلكترونية" – والتي يمكن استخدامها من طرف الغير، وهذا في كثير من الأحيان دون علم صاحبها. ومن ثم فقد ظهرت الحاجة إلى مراعاة الجانب المتعلق باحترام الحرّيات العامة في مواجهة التكنولوجيات الرقمية منذ بداية وجود شبكة الإنترنت. وفي هذا السياق كتب " جون بيري بارلو" أحد مؤسسي منظمة الحدود الإلكترونية E.F.F[1] إعلان استقلال الفضاء الرقمي في 8 فيفري 1996 في دافوس بسويسرا. حيث يدعم فكرة أنه لا يمكن لأي حكومة (أو أي شكل آخر من أشكال السلطة) أن تفرض نفسها وتتملك شبكة الإنترنت، والتي كانت تشهد توسعا كبيرا في تلك الفترة. وفي الآونة الأخيرة، أكد إعلان مبادئ جنيف الذي اعتمده مؤتمر القمة العالمي لمجتمع المعلومات (SMSI)[2] في 12 ديسمبر 2003 صراحة أن حرية الرأي والتعبير تشكل القاعدة الأساسية لمجتمع المعلومات، وبالتالي تطبيق المادة 19 من الإعلان العالمي لحقوق الإنسان على الإنترنت. ويشير النص أيضا إلى أن حرية الإعلام وسيلة لتحقيق مجتمع المعلومات.

---

[1] Electronic Frontier Foundation: https://www.eff.org.

[2] القمة العالمية حول مجتمع المعلومات (بالإنجليزية: World Summit on the Information Society WSIS) هو مؤتمر برعاية الأمم المتحدة عن المعلومات والاتصالات. عقدت القمة مرتين: المؤتمر الأول في ديسمبر 2003 في جنيف. والمؤتمر الثاني في نوفمبر 2005 في تونس(SMSI).

لقد عرّف مجلس الدولة الفرنسي النظام الرقمي على أنه تمثيل للمعلومة أو الكميات الفيزيائية (الصور والأصوات) بواسطة عدد محدود من القيم المنفصلة، التي تمثل في معظم الأحيان ثنائي بتسلسل في العد المعتمد على القيمتين 0 و 1. وتعود قوته التحويلية إلى القدرة على التعبير عن حقائق متباينة (الأصوات والصور والنصوص والسلوكيات البشرية والعمليات الصناعية...) بلغة مشتركة عالمية تمكّن من معالجتها بطريقة آلية وربطها ببعضها البعض. ويؤدي ذلك إلى تحوّلات تقنية واقتصادية واجتماعية[1].

فعلا فمع تطور مجتمع المعلومات، انتقلنا من إدارة الوثائق الورقية إلى إدارة قواعد البيانات الرقمية الكبيرة. إن جميع أنشطتنا اليوم تتكون من عنصر معلوماتي الذي يعبر من خلال الشبكات الرقمية، سواء كنا بصدد الاتصال أو السفر أو الاستهلاك. وبهذا المعنى فإن الإنترنت تتمتع بقيمة المرفق العام. إن البيانات الشخصية[2] التي يتم جمعها وتحليلها تتخذ أشكالا عديدة، ناتجة عن وضع أنظمة المراقبة بالفيديو[3]، والتنصت على الهاتف، والاستخدام المتزايد للشبكات الاجتماعية، وتحديد الموقع الجغرافي أو تطوير التجارة الإلكترونية.. وقد تفاقمت المنازعات المتعلقة بحرمة الحياة الخاصة مع انتشار تكنولوجيا المعلومات ودمقرطة استخدام الإنترنت والهاتف النقّال، ومؤخرا أدوات اتصال و وخدمات رقمية أخرى. هذه التقنيات التي تحتفظ في ذاكرتها بالاستخدامات التي يقوم بها

---

[1] Conseil d'Etat, Étude annuelle 2014:Le numérique et les droits fondamentaux, la documentation française, p.3.

[2] Agathe Lepage, « Liberté et droits fondamentaux à l'épreuve de l'internet », Litec, Paris, 2002, n° 48.

[3] المرسوم الرئاسى رقم 228 - 15 المؤرخ فى 22 أوت 2015 و الذي يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو.

الفرد، تولّد آثارا، وبالتالي تعيد النظر في الحدود الفاصلة بين العام والخاص، وكذلك في نطاق الحريات العامة.

وهكذا أصبح التعبير عبر الإنترنت حاملا لمعلومات يمكن استخدامها بدرجات متفاوتة التطفل. ولكن التعليقات المنشورة على الإنترنت قد تكون أيضا عرضة لانتهاكات أخرى بناءا على محتواها. وفي حين يبدو من المنطقي أن حرية التعبير لا يمكن ممارستها دون حدود وعلى حساب حقوق الآخرين، فإن التوترات المتعلقة بحرية التعبير، والاتصال، والإعلام تظهر بشكل أكبر، حيث أنه تحت مبرر مكافحة الجريمة الالكترونية والإرهاب الإلكتروني، وبهدف عام متمثل في الحفاظ على النظام العام، تتدخل السلطات العمومية في المحتويات المنشورة لمراقبتها أو رصدها أو تقييدها أو حظرها. والنتيجة هي أنه حتى في الدول التي تعتبر تاريخيا نماذج للديمقراطية، مثل الولايات المتحدة الأمريكية، حيث تمارس حرية التعبير بطريقة واسعة جدا وغير محدودة تقريبا، لا تتخلى هذه الأخيرة عن درجة معينة من الاشراف للدفاع عن سياساتها في مجال المراقبة ولا سيما في سياق مكافحة الإرهاب.

وبالنظر إلى تعدد المصادر، فإن النهج الذي يهدف إلى تعريف الحريات العامة يصطدم بسرعة بصعوبات حقيقية بسبب تنوع المفردات الذي تقدمه النصوص المعنية. غير أن الحريات العامة قد تطورت كفئة قانونية مستقلة داخل المجتمع الحديث، رغم أنها كثيرا ما تتهم بأنها تشكل فئة غير واضحة وغير منظمة.

وهكذا وتبعا للسياق الذي توجد فيه قد تكون لبعض الحريات طبيعة هجينة تدخل على سبيل المثال في إطار الحريات الاقتصادية، وكذا في إطار الحريات القائمة على القيم المدنية أو الإنسانية أو الاجتماعية. وهو حال الحق في الملكية، وحرية الصحافة، وحرية التعبير، وحرية التنقل، وحرية التعاقد، أو مبدأ عدم

التمييز. وفي هذا السياق، يتم الكشف بسرعة عن الطبيعة المتغيرة لحقوق الإنسان والحريات العامة عندما ندرك أن نفس الحق، ونفس الحرية، يمكن الاحتجاج بها لتبرير إما غايات تجارية وإما مدنية أو إنسانية.

بصفة عامة لقد صيغت فكرة الحريات العامة في البداية كقيد على الحكام في مواجهة صلاحيات السلطات الثلاث (السلطة التشريعية والتنفيذية والقضائية) من أجل تقديم ضمانات الأمن والحرية للمواطنين. إن مفهوم الحريات العامة بدأ في أشكاله المختلفة في القرن الثامن عشر على إثر الثورات الإنكليزية والأمريكية والفرنسية، وقد تجسدت فيما بعد في إعلانات حقوق الإنسان والدساتير التي أصبحت المصادر الأساسية لها. لقد أصبحت الدساتير اليوم من أهم الضمانات للحريات العامة المنصوص عليها صراحة إذ قررت الإجراءات المترتبة عن الإخلال بها في نصوصها العقابية ومن ذلك الدستور الجزائري لسنة 1996 (حرية الرأي العام وحرية المعتقد م36، حرية الإبتكار وحرية الفكر التقني والعلمي م 38، حرية التجارة والصناعة م 37، حرية التعبير وإنشاء الجمعيات السياسية والإجتماع، حرية الإنتقال والتنقل م 44).

وعلى عكس الفرضيات التي طالما سعى رواد الإنترنت إلى ترسيخها، مطالبين بالحرية الكاملة على الانترنت والاتصال بلا حدود ودون تدخل حكومي، أصبح من الجائز عموما حاليا وبهدف مكافحة السلوك غير المشروع ودعم تطور الإنترنت، أن تلجأ الحكومات إلى مبادرات تشريعية وتنظيمية مناسبة. ليست الانترنت إذن بأي حال من الأحوال فضاء بلا قانون[1]، أو منطقة منفصلة عن الحيز المادي، لأنه حتى ولو كانت الأعمال فيها افتراضية، فإن آثارها حقيقية وملموسة من طرف أشخاص طبيعية ومعنوية. في نهاية المطاف فإنه وراء كل

---

[1] JACQUES LARRIEU / وترجمة د. محمد سيد توفيق، قانون الانترنت، المنظمة العربية للتنمية الإدارية،الطبعة الاولي، القاهرة، 2009، ص 10.

حاسوب يوجد إنسان لا ينبغي أن تمر أعماله غير المشروعة دون عقاب. وإن تطوير التجارة الإلكترونية[1] بصفة قانونية يعتمد أيضا على تبني قواعد من شأنها أن تضمن للشركات والمستهلكين مبادلات تجارية ومدفوعات بشكل عادل وفعال. كما هو الحال مع وسائل الإعلام التقليدية، يمكن أن تكون الإنترنت ويجب أن تكون موضوع تنظيم حكومي معتمد على المستوى الوطني أو من خلال المنظمات الدولية.

إذن ليست فقط قواعد القانون الجزائي والمدني والتجاري التقليدية التي تطبق على الانترنت، ولكن أيضا قوانين أخرى تأتي لتعزيز الأحكام القائمة وتدارك النقائص إن وجدت. وهكذا تم اعتماد قوانين لمكافحة الهجمات الإلكترونية، وإدارة التجارة الإلكترونية والإعلان عبر الإنترنت، وتحيّين نظام معالجة البيانات الشخصية، وحماية الإبداعات الفكرية على شبكة الإنترنت، ومكافحة المواد الإباحية المتعلقة بالأطفال وتكيّيف إجراءات التحقيق التي تطال الشبكة. يضاف إلى كل ذلك القواعد الدولية من خلال الاتفاقيات كاتفاقية بودابست لمكافحة الجرائم المعلوماتية الموقعة في 23 نوفمبر 2001 تحت رعاية مجلس أوروبا.

ولكن هذه القواعد المختلفة تتسم بتناقضات عدة. من جهة يقدم الإنترنت بشكل منهجي باعتباره خطر خارجي يجب فيه حماية المواطنين، وكذلك تسعى الدولة إلى الاستفادة من التتبع وتستخدم نفس تقنيات المراقبة التي يستخدمها الخواص، تحت ذريعة الرغبة في التصدي لخطر الانحراف والإرهاب. في اطار هذا المنطق الأمني يتم الجمع بين تنظيم بوليسي مفرط وتحرير السوق. مسألة القانون لا يتم التطرق إليها إلا تحت زاوية تكيّيف القواعد القديمة مع بيئة وأدوات

---

[1] مصطفى يوسف كافي، التجارة الإلكترونية، دار رسلان للطباعة والنشر والتوزيع، الطبعة الاولي، دمشق، 2009.

جديدة. ونتيجة لذلك لا تمارس الحقوق الأساسية في الفضاء الرقمي – رغم أنه صمم من أجل ذلك – ولكن كثيرا ما ما يتم تجاهلها.

يجب إذن على المشرع البحث عن "الأمن الجماعي" على الشبكة والذي من شأنه التوفيق بين مختلف الحقوق الأساسية والمتضاربة في جزء منها، مثل حرية التعبير والحق في حرمة الحياة الخاصة وحق الملكية، الخ. لذلك لا ينبغي اغفال أنه بقدر ما كان للفرد الحق في الحماية من الجريمة والإرهاب – التي تلتزم الدولة بضمانها، لديه الحق أيضا في حماية حريته في التعبير والاعلام وحماية بياناته الشخصية وحياته الخاصة – التي تلتزم الدولة بضمانها أيضا.

ولكن هل المراقبة الرقمية التي جاء بها المشرع اجراء مشروع لمواجهة النزعة الإجرامية بصفة عامة والارهابية بصفة خاصة؟ أم أنه إعتداء صارخ على الحريّات العامة، خاصة ما تعلق منها بحرية التعبير وحرمة الحياة الخاصة؟ كيف يتم التطبيق الفعلي لقواعد حماية الحريات العامة للأفراد في الفضاء الرقمي غير المرئي؟ هل يجب مهما كلّف ذلك محاولة تطبيق القانون القائم ؛ تكيّيفه ليشمل الاستخدامات الرقمية ؛ أو تصور أنظمة جديدة على افتراض أن الآليات التقليدية تختلف كثيرا عن كيفية عمل الفضاء الرقمي؟ بغض النظر عن هذه التساؤلات، كيف نواجه الخصوصيات التقنية لهذا الوسط (النشر بلا حدود، المساس بحرمة الحياة الخاصة تسهله التكنولوجيا، إفلات من العقاب يعززه التستر)؟

للجواب على هذه الاشكالية سنتطرق في الفصل الأول من هذا البحث إلى تحليل الحوار بين من جهة، المفاهيم المتجددة للحريات العامة من خلال استخدام شبكة الانترنت، والأخطار التي تشكلها هذه الممارسة من حيث السلوكيات المسيئة. وبالتالي سنحاول تحديد معالم جديدة للحريات العامة – وبشكل خاص حرية التعبير والاتصال والاعلام، والحق في حرمة الحياة الخاصة وسرية

البيانات الشخصية – من خلال الخصائص التقنية والقانونية التي يتميّز بها الوسط الرقمي. على هذا النحو ينبغي أن نأخذ بعين الاعتبار أن التحليل سوف يقتصر على عدد من الحريات العامة التي تبدو لنا مهمة على نحو خاص، على الرغم من أن حريات أخرى يمكن أن تكون أيضا موضوعا لهذا البحث(فصل أول).

سنتطرق في مرحلة ثانية إلى الضمانات الضرورية لحماية الحريات الرقمية ونختم هذا البحث بالحديث عن دور القضاء في حماية هذه الحريات(فصل ثاني).

وقد خلصنا في الأخير إلى ملاحظات واقتراحات شملتها الخاتمة.

الفصل الأول

الانترنت فضاء جديد لممارسة الحريات العامة تحت المراقبة

إن الإنترنت باعتبارها فضاء للاتصال ترتبط بصفة مباشرة أو غير مباشرة بالعديد من الحريات العامة و الحقوق الأساسية. في الواقع، بما أن تأطير وسائل الاتصال الالكتروني من اختصاص الدول، ولو بصفة جزئية رغم الخصائص الاقليمية لعمل الشبكة، فإن الالتزامات الدولية الموقعة فيما بينها في مجال حماية الحقوق تطبق منطقيا. لا تكون دائما ممارسة هذه الحريات على أساس نفس المبادئ المطبقة على وسائل الاتصال التقليدية.

رغم أن الحريات الرقمية مازالت تشكل الغائب الأكبر في الدساتير العربية و حتى الأوروبية منها إلا أن المفوضية الأوروبية إعتبرت في الفترة الأخيرة أنها تدخل في إطار معايير "كوبنهاغن". و هذا يعني أن إحترام الحريات الرقمية من طرف الحكومة يعد شرطا من شروط قبول العضوية في الاتحاد الأوروبي[1].

و إعتبر الاتحاد الأوروبي في التقرير المتضمن بناء استراتيجية من أجل الحرية الرقمية في السياسة الخارجية للاتحاد الأوروبي "أن الحريات الرقمية هي حقوق أساسية و هي ضرورية من أجل ممارسة حقوق الانسان التقليدية كحرية التعبير و حرية التجمع و كذلك من أجل ضمان الشفافية و المسؤولية في الحياة العامة"[2].

و هكذا فإن الحريات العامة تحت تسمياتها المختلفة مثلها مثل حقوق الانسان الالكترونية كما سماها " تيم بيرنرز لي" مخترع الإنترنت[3]، برزت كإشكالية أساسية في آلية عمل شبكة الأنترنت.

---

[1] جواب المحافظ الاوروبي ستيفان فول المكلف بالتوسيع وسياسة الجوار الاوربية عن سؤال لنائب أوروبي مدافع عن الحقوق الرقمية في أوروبا بتاريخ 2011/06/01 تحت رقم E-005344/2011 في إطار مفاوضات انضمام دولة تركيا للاتحاد الأوروبي، حيث اعتبر أن الحريات الرقمية بما فيها حرية التعبير والإعلام من أهم القيم الأوروبية و تدخل في شروط بداية أي مسار انضمام للاتحاد الأوروبي.

[2] تقرير النائبة الهولندية "ماريتجه شاكه" في لجنة الشؤون الخارجية في البرلمان الأوروبي رقم 2012/2094(INI).

[3] Tim Berners-Lee, « Long Live the Web », Scientific American (2010) 303, n° 6, p. 80-85.

الضمان الفعلي للحريات العامة في العالم الرقمي.

أدت وسائل الاعلام و الاتصال وخاصة الإنترنت إلى تعديل السياق المكاني الذي تجري فيه الأنشطة الانسانية. حيث توظف في الواقع الرقمي مفردات تشير إلى المكان و الفضاء مثل المواقع، البوابات، المنتديات، غرف الدردشة، وطريق المعلومات السريع[1]، و تستخدم هذه الألفاظ على سبيل المجاز ولا تعكس أي امتداد للواقع الحقيقي إلى الفضاء الافتراضي. لذا فإنه يصبح لزاما على نظام حماية الحريات العامة التكيّف حاليا مع تطور وسائل الاعلام و ضرورة إيجاد تطورات جديدة في قانون الانترنت حيث تؤدي كل وسيلة إلى تحليل المبادئ المطبقة بألفاظ جديدة. مما لا شك فيه أن المجالات الأكثر تأثرا بظهور تكنولوجيا الاتصال الحديثة هي حرية التعبير والاتصال و حرمة الحياة الخاصة. في حين أن حرية التعبير و الاتصال وما ينبثق عنها من حرية الرأي و المعتقد و الاعلام، تؤطر حرية نشر و تدفق المحتوى الرقمي (مطلب أول) أدى إلى تغيير عميق يظهر من خلال مجموعة من الممارسات (مطلب ثاني)، أما الحق في حماية البيانات الشخصية والحق في سرية الاتصالات فهي حقوق تسمح بتجسيد الجانب الشخصي في الفضاء الرقمي (مطلب ثالث).

إعادة تحديد أطر الحريات العامة في المجال الرقمي.

في ظل التغييرات التي شملت الحريات العامة في العالم الرقمي، نطرح مجموعة من التساؤلات المتعلقة على حد السواء: بطبيعة القواعد التي تحكم

---

[1] Thierry Vedel, « Les politiques des autoroutes de l'information dans les pays industrialisés: une analyse comparative », Réseaux, 1996, n° 78, p. 11-28.

ممارسة الحريات العامة في السياق الرقمي (فرع أول) والاعتراف بالتحولات التي طرأت على المفاهيم المتعلقة بالحريات العامة مع التمييز بين حرية التعبير و حرية الاتصال (فرع ثاني) و حرية الاعلام (فرع ثالث).

الآثار القانونية لتكنولوجيا الاتصال الحديثة على الحريات العامة.

إن النصوص التشريعية التي صدرت دفاعا عن حرية الصحافة والسابقة لظهور الإنترنت، نرى بعضا من أحكامها يطبق مباشرة. لكن البعض منها تم تعديلها من أجل التأطير القانوني للغزو الذي شهده قطاع النشر عبر وسائط غير مادية افتراضية[1]. لكن هذه القواعد تبقى غير كافية وبما أن الأمر يتعلق بتكنولوجيا الاتصال الرقمي، كان بالإمكان التفكير في قواعد قانون الاتصال السمعي البصري التي من شأنها أن تكون الأكثر ملائمة. في الواقع فإن التلفزيون كوسيلة أساسية للاتصال السمعي البصري يتقارب مع الإنترنت في خصوصياته التقنية، بالنظر لانتشاره الواسع في المجتمع. لذا فإن العديد من الدول تنظم عموما قطاع السمعي البصري من خلال سن قانون، وهناك أحيانا حتى من تضمنه في النص الدستوري.

على هذا النحو وعلى سبيل المثال فإن محكمة التحكيم البلجيكية اعتبرت أن البرامج التلفزيونية يمكن أن تخضع دستوريا للرقابة وذلك حماية للشباب. إعتبرت أن محتوى هذه البرامج يمكن أن يخضع للرقابة من طرف سلطة إدارية من دون أن يكون هناك مساس مفرط بحرية التعبير.

---

[1] صدرت في فرنسا مجموعة من القوانين المنظمة للصحافة الالكترونية: المرسوم رقم 2007-1527 الصادر في 24 أكتوبر 2007 المتعلق بالحق في الرد الالكتروني ؛ المرسوم رقم 2009-1340 الصادر في 29 أكتوبر 2009 المتعلق باصلاح النظام القانوني للصحافة ؛ المرسوم رقم 2009-1379 الصادر في 11 نوفمبر 2009 المتعلق بصندوق دعم خدمات الصحافة الالكترونية.

أما المشرع الفرنسي فإنه فضّل الذهاب أبعد من ذلك. حيث ظهرت طائفة جديدة من القواعد بجانب قانون الصحافة المكتوبة و قانون السمعي البصري. وجاء قانون 575/2004 المتعلق بالثقة في الاقتصاد الرقمي[1] و أكّد في المادة الأولى منه على إنشاء فئة عامة جديدة: "اتصالات عامة عن طريق الوسائل الالكترونية"، و تنقسم إلى "اتصالات السمعي البصري" و اتصالات عامة على الانترنت". و قد عرفت المادة 02 من نفس القانون "الاتصالات العامة على الانترنت " على أنها " كل ما يوضع في متناول الجمهور أو فئة منه، عن طريق الاتصال الالكتروني، من علامات وإشارات وكتابات وصور وأصوات أو رسائل من أي نوع كان لا يكون لها طابع مراسلات خاصة[2].

وهذا يقودنا الى ملاحظتين هامتين. من جهة، يمكن أن يكون للمحتوى الرقمي طابع عام (منشورات على المدونات و منتديات الدردشة...) أو خاص (رسائل البريد الإلكتروني، المنشورات المحمية بوسيلة تحقق من الهوية أو بكلمة المرور...). عندما لا يكون للمحتوى طابع مراسلة خاصة، يعتبر موجها للعامة.

من جهة أخرى، متى كانت المحتويات عامة تكون التفرقة عموما بين ما ينتمي منها إلى الاتصالات العامة على الانترنت وما ينتمي منها إلى الاتصالات السمعية البصرية.

يمكننا أن نلاحظ على نحو متزايد تجانس قانون الإعلام بتحديد عامل مشترك لجميع الأحكام المطبقة على جميع خدمات الاتصالات العامة الإلكترونية مقابل المراسلات الخاصة. و بذلك تم نسخ مبادئ حرية الاتصال واستثناءاتها الواردة

---

[1] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JO n°143 du 22 juin 2004, p.11168.

[2] ويؤدي الفصل بين هذين النظامين، أي الاتصال السمعي البصري والاتصالات الالكترونية، إلى وضعهما تحت سلطة رقابة مختلفة. وهكذا، في حين أن هيئة التنظيم للاتصالات الإلكترونية والبريد هي المسؤولة عن الأنشطة المتعلقة بالاتصالات الالكترونية، والمجلس السمعي البصري يبقى مختصا فيما يتعلق بالاتصالات السمعية والبصرية.

في المادة 01 من قانون 30 سبتمبر1986 المنظم للاتصالات السمعية البصرية وتم إدراجها في القانون المنظم للإنترنت. ونفس الشيء بالنسبة للتعريفات الأساسية. و هكذا سيتم التعامل بطريقة موحدة مع جميع المسائل المشتركة لوسائل الاعلام والخدمات، بغض النظر عن طريقة وضعها في متناول الجمهور، مثل المركز القانوني للصحفي أو المسؤولية التحريرية. في بعض الدول وصل تجانس القواعد بين الاتصالات العامة على الانترنت و الاتصالات السمعية البصرية إلى درجة أن تنظيمها قد أسند إلى هيئة واحدة.

إيطاليا كانت من الدول الرائدة بإنشائها سنة 1997 لهيئة ضبط مستقلة لقطاع الاتصالات[1] و الذي تضم الاعلام والاتصال، السمعي البصري (اذاعة، تلفزة، وسائل الإعلام الجديدة) و الصحافة المكتوبة. في بريطانيا هناك هيئة ضبط وحيدة[2] و تغطي الاذاعة، والاشهار، والإنترنت، والاعلام و الاتصال والصحافة المكتوبة. في فنلندا يوجد سلطة ضبط الاتصالات[3] وهي أيضا هيئة ضبط وحيدة، مسؤولة عن المسائل المتعلقة بالاتصالات الإلكترونية (بما فيها التلفزة والاذاعة) وعن خدمات مجتمع الاعلام. وفي الأخير في الولايات المتحدة الأمريكية هناك اللجنة الفدرالية للاتصالات[4] مكلّفة بضبط الاتصالات، والاذاعة، والتلفزة و الأنترنت. و لكن تبقى رقابتها على المحتوى محدودة بفعل التفسير الواسع النطاق لمعنى حرية التعبير المكرسة في البند الأول من الدستور الأمريكي.

---

[1] L'Autorità per le garanzie nelle comunicazioni (**AGCOM**).

[2] L'**Ofcom** (Office of Communications).

[3] **FICORA** (Finnish communications regulatory authority).

[4] The Federal Communications Commission (**FCC**) is an independent agency was formed by
the Communications Act of 1934.

لذلك و رغم مظهرها كوسيلة إعلام جديدة، يتم استغلال الإنترنت أيضا كدعّامة جديدة لوسائل الإعلام الكلاسيكية الثلاث. و الواقع أن ما يسمى بالوسائط المتعددة يتطلب توظيف جميع وسائل الإعلام الكلاسيكية: من كتابة، وصوت، و صورة.

يجب إذن تكييف الأنظمة القانونية لأن القوانين القائمة على التمييز وفقا لنوع المحتوى السمعي البصري، تفقد أهميتها في ظل التقارب الرقمي التدريجي.

تطور حرية التعبير و الاتصال في إطار الواقع الرقمي.

يستند قانون الاتصال على عدة جوانب من الحريات العامة من دون تحديدها بصفة حصرية. حرية التعبير (أولا) بالاضافة إلى حرية الرأي (ثانيا) تشكل جوهره. لا يتعلق الأمر هنا فقط بحرية التعبير عن أفكاره، أو عن آرائه، أو معتقداته (تظهر هنا أهمية حرية المعتقد)، سواء بالقول، أو بالكتابة، أو بالصورة، أو بالاشارة، أو بموقف معين، أو بكل الطرق الحديثة لاستنساخ ونشر الفكر والكلمة، ولكن أيضا في الحق في البحث عنها وتلقيها.

أولا: حرية التعبير والاتصال بالمعنى الدقيق للكلمة.

بما أنها حرية يعتمد إتساعها على القانون، فإن حرية التعبير و الاتصال هي حرية سياسية. ومع ذلك فهي أيضا وثيقة الصلة بحرية الفكر و حرية الصحافة[1]. و قد ذكر مبدأ حرية التعبير لأول مرة من قبل البريطاني جون ميلتون في كتابه Areopagitica. في خضم الثورة الانجليزية، دافع هذا الكاتب عن حرية

---

[1] إيمانويل كانط في "ما هي الأنوار؟" يدافع عن الأطروحة القائلة بأن حرية التعبير يجب أن يكفلها القانون بغرض تطوير الإنسانية.

الصحافة بقوله: « *Give me the liberty to know, to utter and to argue freely according to conscience, above all liberties* »[1] .

هذا الكتاب سوف يلهم محرري الدستور الأمريكي عام 1791، بإدانتهم دون قيد أو شرط، " لكل قانون يحد من حرية التعبير"[2] الطابع الأساسي لحرية التعبير يكمن في أنها، من جهة، تتمتع بحماية دستورية[3] و دولية[4]، و من جهة أخرى تلزم المشرع وليس فقط الادارة. وأخيرا فإنها تنتج آثار قانونية في العلاقات بين الأفراد وليس فقط بين الأفراد والحكومة، أي أن لديها "أثر أفقي".

حرية التعبير والاتصالات التي تتيح لأي شخص أن يعبّر بحرية عن أفكاره بكل الوسائل التي يراها مناسبة، يعتبرها بعض الفقه بأنها " حق خارج عن المألوف "[5]. حيث تؤدي دورا جوهريا في نظام الحقوق الأساسية، وهذا من

---

[1] ترجمة: "أعطني الحرية كي أعرف، أن أنطق، وأقول بحرية ما يوافق ضميري فوق كل الحريات". J. Milton, Areopagitica, A Speech For The Liberty Of Unlicensed Printing To The Parliament Of England », The Lawbook Exchange Ltd., 1890.

[2] البند الأول من الدستور الأمريكي (First Amendment)، 25 سبتمبر 1789 (المصادق عليه في 15 ديسمبر 1791) ينص على « Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances » (يحظر على مجلس الكونغرس تشريع أي قانون يؤدّى إلى دعم ممارسة أى دين، أو تشريع أى قانون يؤدّى إلى منع ممارسة أى دين ؛ أو تشريع أي قانون يؤدّي إلى تعطيل حرية الكلام أو النشر الصحفي أو حق الناس في إقامة تجمعات سلمية أو إرسالهم عرائض إلى الحكومة تطالبها برفع الظلم.)

[3]

[4] Article 10 de la CEDH, art ; 19 de la DUDH, etc.

[5] Frédéric Sudre, « Droit européen et international des droits de l'homme », PUF, coll. « Droit fondamental », 7e éd., p. 451.

ناحيتين. أولا أنها حرية أساسية في سير المجتمع الديمقراطي[1]. بعض الفقهاء يعتبر حتى أن ممارسة حرية التعبير هي السمة المميزة للحياة الديمقراطية، والتي تسمح بإثبات وجود رأي عام ومجتمع مدني[2]. وبضمان وضوح النقاش الديمقراطي، فإنها تساهم في إحترام مبدأ سيادة القانون. ثانيا وعلى المستوى الفردي، فإنها تسمح بتطوير وتنمية الفرد. في الواقع وباعتبارها شرطا لحرية الفكر فإن حرية التعبير مظهر من مظاهر الاستقلالية الفكرية للأفراد وتحدد علاقاتهم مع الغير ومع المجتمع. وعلاوة على ذلك وبالنظر إلى تطور التجارة الإلكترونية، يمتد التمتع بهذه الحرية أيضا إلى الشركات التي تمارس أنشطتها على الإنترنت. في نفس هذا الاتجاه فإن حرية التعبير هي أساس القانون الأوروبي لأنها أصل حرية تنقل السلع والأشخاص وحرية إنشاء وتوفير الخدمات.

عموما وبما أن وجود الانترنت يشكل اليوم عاملا أساسيا في تطوير العلاقات التجارية، فإن احترام حرية التعبير عنصر أساسي لتمكين الشركات من الترويج لمنتجاتها وخدماتها بشكل مسؤول.

في الأخير فإن حرية التعبير هي حجر الزاوية بالنسبة للشركات التي تنشط في مجال وسائل الإعلام والصحافة، لأنها تعتمد عليها لإنتاج المحتوى الاعلامي، كما أنها عامل تسلية وتمثل أداة رقابة في مواجهة الحكومات. كمنصات

---

[1] CEDH, 7 déc. 1976, Handyside c/ Royaune-Uni, v. n° 5493/72.

[2] Henri Oberdorff, « Droits de l’Homme et libertés fondamentales », 2ème éd., LGDJ, n° 395 ; Etienne Montero et Quentin Van Enis, « Ménager la liberté d’expression au regard des mesures de filtrage imposées aux intermédiaires de l’Internet: La quadrature du cercle ? », RLDI, mai 2010, n°60, p. 88.

التكنولوجيا على سبيل المثال التي توفر لمستخدميها فرصة تبادل وجهات النظر على الانترنت.

أدى التقدم التكنولوجي في أواخر القرن العشرين وأوائل القرن الحادي والعشرين الذي سمح بإنشاء شبكة الإنترنت في الواقع إلى تطوير شبكة اتصالات عالمية تمنح الفرد إمكانية مخاطبة أوسع جمهور ممكن. قياسا على طريقة تطوير أول أجهزة الكمبيوتر الشخصية، يمكن أن نعتبر أن حرية التعبير في السياق الرقمي هي حرية الفرد في مرآب منزله الذي يريد إطلاق موقع جديد أو مدونة جديدة، في إمكانية اعتماده على الإنترنت لتقديم محتوى عمله إلى العالم. في نفس السياق فإن الإنترنت تشكل قيمة لا تقدر بثمن كمورد عام عالمي. حيث أنها توسع وبشكل جذري فضاء التعبير والاتصال في جميع أنحاء العالم، ولم تعد موردا نادرا[1]. فهي على شاكلة " أغورا " عالمية تتجاوز تعقيدات الحدود الجغرافية[2] التي شارك فيها 2.749 مليار مستخدم في عام 2013، ما يقرب 40٪ من سكان العالم[3].

هناك بصفة عامة علاقة تكاملية بين الإنترنت وحرية التعبير وذلك لأن حماية واحترام حرية التعبير على شبكة الإنترنت تُمكّن هذه الأخيرة من الحفاظ على فائدتها الأساسية، أي الحفاظ على شكل شبكة محايدة والتي تربط بين

---

[1] Pierre-François Docquir, « Le « droit de réponse 2.0 » ou la tentation d'un droit subjectif d'accès à la tribune médiatique », Revue de Droit de l'U.L.B., n° 35, 2007.

[2] أ.رضوان قطبي، الديمقراطية الرقمية في الوطن العربي: واقع وآفاق، دنيا الوطن،-2015-11-01.

[3] V. Union Internationale des Télécommunications, rapport « Mesurer la société d'information ».un résumé analytique disponible à l'adresse: http://www.itu.int/en/ITUD/Statistics/Documents/publications/mis2013/MIS2013-execsum_F.pdf.

الأشخاص في جميع أنحاء العالم، دون أن تخضع للتدخل من أي سلطة لغرض التأثير على المحتوى الرقمي. فعّالية هذا الحياد هو سبب وجود الإنترنت لأنه من خلال هذا الحياد والاستقلالية والطابع العالمي الموصولين بها، يتم استخدامها من قبل عدد كبير و متزايد من الناس. إن لم تكن الإنترنت توفر اتصالات دون رقابة، لفقدت جزءا كبيرا من فائدتها، ولم يكن لها أبدا أن تصبح ما هي عليه اليوم: أي الوسيلة الأساسية لتبادل المحتوى في العالم ورمزا للشفافية بامتياز. و تكمن قوتها التي تميّزها عن طرق الاتصال الفكرية الأخرى، أنها تشكل "مساحة جديدة للتعبير، وفضاءا إفتراضيا ليس له حدود، و لا نهر يحده، ولا سلطة مركزية تتحكم فيه".[1]

وجدت حرية التعبير على الإنترنت بالمقابل شكلها الكامل، بالسماح للجميع بإنشاء موقع ويب، مدونة شخصية، أو غيرها من خدمات الاتصالات عبر الإنترنت، و لكن أيضا بتقديم محتويات رقمية عبر المنصات، والتسجيل على شبكة اجتماعية، والمشاركة في البرمجيات التعاونية بكل حرية، الخ.

المواقع المنشورة على الشبكة ليست موجهة لفرد بعينه والوصول إليها من حيث المبدأ متاح للجميع، بغض النظر عن إعتبارات المسافة أو الجنسية أو مكان الإقامة. وبالتالي يكون التواصل دون الأخذ بعين الاعتبار للحدود السياسية بين الدول. هذه الحرية أيضا مشروطة بالحق في التعبير من عدمه عن المعتقدات الدينية أو الآراء السياسية أو الانتماء إلى فئة أو مجموعة إثنية أو عرقية. و لذلك

---

[1] Limore Yagil, « Internet et les droits de la personne, nouveaux enjeux éthiques à l'âge de la mondialisation », Les éditions du CERF, Paris, 2006, p. 55.

فإن ممارسة حرية التعبير المتاحة عن طريق وسائل تكنولوجيا المعلومات تسمح بممارسة مجموعة كاملة من الحريات العامة الأخرى[1]. ممارستها تشمل على سبيل المثال، ممارسة التعبير الفني. كما جاء في قرار محكمة حقوق الإنسان الأوروبية، "أولئك الذين ينتجون أو يؤدون أو يوزعون أو يعرضون الأعمال الفنية يساهمون في تبادل الأفكار والآراء الضرورية لوجود مجتمع ديمقراطي"[2].

ثانيا: الحريات المرافقة: حرية الرأي وحرية المعتقد.

بالمثل، يمكن أن تندرج حرية الفكر والضمير والرأي تحت تسمية حرية التعبير كلما تعلق الأمر بالتعبير، بتجسيد أفكار أو معتقدات أو آراء[3]. الفقهاء يعّرفون بدورهم حرية الرأي على أنها "حرية تكوين رأي حول أي موضوع، و نشره و تلقي رأي الآخرين". وعلاوة على ذلك، و لامكانية ولادته يحتاج الرأي أن يكون مبنيا على حقائق، لذا ينبغي أن يُدرج في نطاق هذه الحرية: حرية البحث ونشر والحصول على المعلومات.

تندرج حرية الرأي في طليعة المبادئ التي تعتمد عليها المحكمة الأوروبية لحقوق الإنسان، و ذلك منذ قرار "ليجنس" ضد النمسا في 8 يوليو 1986.

---

[1] Ahmed Dahmani, José Do-Nascimento, Jean-Michel Ledjou, Jean-Jacques Gabas, « La Démocratie à l'épreuve de la société numérique », éd. Karthala, Paris 2007, p.375.

[2] CEDH, Müller et autres c/ Suisse, 24 mai 1988, n° 10737/84.

[3] لكن في بعض البلدان تختلف حرية المعتقد عن حرية التعبير وبالتالي فهي محمية بشكل مستقل. وهكذا وطبقا للقانون الأساسي النمساوي المؤرخ في 21 ديسمبر 1867 المتعلق بالحقوق العامة للمواطنين في الممالك والبلدان الممثلة في مجلس الإمبراطورية فإنه على الرغم من أن حرية التعبير هي حرية المعتقد والوجدان، فإن الحق في المعتقد غير محمي على نفس الأساس: "إن التمتع بالحقوق المدنية والسياسية مستقل عن الانتماء إلى دين معين" (المادة 14). وهو نفس المنطق الذي تبناه المشرع الجزائري في نص المادة ٣٦ من الدستور.

تشكل الإنترنت وسيلة خاصة للتعبير، لدعم قضية للنضال دون أن يكون الشخص مجبرا على الانتماء إلى حركة ما أو نقابة أو جمعية. كل ما يحتاجه هو حساب الفيسبوك ليكون قادرا على ذلك، عن طريق النقر على زر "أعجبني" ("J'aime") لإعلام المستخدمين الآخرين عن مصالحه، وأولوياته، وآراءه، الخ. كما يعتبر مستخدموا الأنترنت منتديات النقاش كأداة للديمقراطية أين تتبلور حرية الرأي التي يطالبون بها.

في هذا السياق تم الاعتراف في حكم صادر عن محكمة الاستئناف الفدرالية في ولاية فرجينيا في 18 سبتمبر 2013[1] بأن التعبير بـــ "أعجبني" ("J'aime") بخصوص موضوع على الفيسبوك و إعتبره جزءا لا يتجزأ من ممارسة حرية التعبير على الإنترنت.

وأخيرا فيما يتعلق بحرية المعتقد، فإن الإنترنت هي بلا شك وسيلة تعبير استثنائية للمعتقدات الدينية لمختلف الطوائف[2]، سواء في سياق "الدين على الانترنت" أو "الدين عبر الإنترنت"[3]. تتيح حرية الاعلام الديني عبر المواقع

---

[1] CA du quatrième circuit, n° 12-167, B. Bland, D.R. Carter Jr, D.W. Dixon, R.W. McCoy, J.C. Sandhofer, D.H. Woodward c/ B.J. Roberts, texte du jugement disponible à l'adresse: http://fr.scribd.com/daoc/169110696/Facebook-4-Th- Circuit.

[2] S. O'Leary, المتخصص الأمريكي في الدين والاتصال، وأحد أول من حلل دور الإعلام الجديد داخل الطوائف الدينية، يقول إن ظهور الإنترنت كان له أثرا ثوريا في تنمية الأديان و انتشارها مثله مثل الأثر الذي أحدثه اختراع الطباعة. V. S.D. O'Leary, « Cyberspace as Sacred Space: Communicating Religion on Computer Networks », Journal of the American Academy of Religion, n° 64, hiver 1996, 781-808.

[3] ويمكن أن تندرج ممارسة حرية الدين عن طريق الإنترنت في إحدى فئتين يحددهما الفقه: "الدين على الإنترنت" و "الدين عبر الإنترنت". وبينما تشير الفئة الأولى إلى البحث عن

الإلكترونية أو المدونات فرصا جديدة للاتصال ليس فقط بالنسبة لأعضاء الطوائف الدينية، ولكن أيضا بالنسبة للأشخاص الذين هم خارج هذه الطوائف. هذا يخلق إذا بعدا جديدا من الشعور بالانتماء و الذي يصبح ممكنا لملايين من الناس الذين يشاركون في "غرف الدردشة" أو ينخرطون في منتديات النقاش.

إن إحترام حرية المعتقد على الأنترنت يشمل احترام حقوق أساسية الأخرى، مثل حرية تكوين الجمعيات. ومع ذلك يمكن أن تكون حرية المعتقد مع حريات أساسية أخرى، و خاصة حرية التعبير. إن السؤال المطروح في الواقع، ما إذا كان على أعضاء جماعة دينية معينة أن يتقبلوا دائما انتقاد دينهم ضمن حرية التعبير المضمونة للجميع في المنتدى العام؟ أم أن حريتهم الدينية تعني تمتع معتقداتهم الدينية بحماية خاصة ضد الخطابات المسيئة التي تحرّض على الكراهية أو التمييز الديني؟ على العكس من ذلك، هل الانتماء إلى جماعة دينية يسمح بالتعبير عن القناعات بكل حرية بلا قيد أو شرط، في حين أن بعض الأفكار قد تنكر حقوق الآخرين أو تتعارض مع القيم الديمقراطية؟ في هذا السياق هناك عدة عوامل تبرر القيود التي يمكن أن تفرض على حرية التعبير، لأسباب دينية: حماية للدين، وحقوق الأفراد والجماعات في المجتمع، أو حماية للنظام أو الأمن العام والديمقراطية أو سيادة القانون.

معلومات عن دين معين على الإنترنت ونشرها، تشير الثانية إلى الممارسة الدينية على الإنترنت.

V. L.L.Dawson, et D.E. Cowan (éds), « Religion Online: Finding Faith on the Internet », New York, Routledge 2004 ; C. Helland, « Online Religion/Religion Online and Virtual Communites », dans « Religion on the Internet: Research Prospects and Promises », J.K. Hadden et D.E. Cowan (éds), London, JAIPress/Elsevier Science 2000.

تطور الضمانات الضرورية لاحترام حرية الاعلام.

الحق في نشر المعلومات و الأفكار هو العنصر الأكثر وضوحا في حرية التعبير[1]. و يشمل الحق في أن نقول ما نفكر به أو ما نعرفه، في حياتنا الخاصة أو في وسائل الإعلام. ولكن حرية التعبير تخدم غرضا أوسع، متى تمكن كل شخص من الحصول على أوسع نطاق ممكن من المعلومات و الآراء، بفضل و من خلال احترام حرية الاعلام. وقد أصبح هذا الحق في الاعلام حقا جديدا، و هو حق متميز لكن لا يمكن فصله عن الحق في حرية التعبير. وحسب تعريف عام، فإن ممارسة حرية الاعلام هي "فعل إيصال بعض الوقائع أو بعض الآراء إلى علم الجمهور بمساعدة الأجهزة البصرية أو السمعية تحمل رسائل واضحة لهذا الجمهور. والخبر هو أيضا نتيجة لهذا الفعل على المخاطبين"[2]. في هذا الاتجاه تتبلور حرية الاعلام في مظهرين: الحق في الإعلام والحق في المعلومة. من جهة فهي حق الصحفي أو المحرر للبحث و نقل الأخبار، و من جهة أخرى "حق الجمهور في المعلومة"، وهذا يعني حق المواطن في أن يعرف، و بالتالي في أن يصل إلى المعلومة[3].

---

[1] كما هي محددة، تشمل حرية التعبير "(...) الحق (...) الحق في تلقي ونقل، دونما اعتبار للحدود، للمعلومات (...)" (المادة 19 من الإعلان العالمي لحقوق الانسان) و "(...) الحق (...) البحث و تلقي و نقل المعلومات والأفكار مهما كانت طبيعتها، دونما اعتبار للحدود، سواء بالقول أو الكتابة أو الطباعة أو الفن، أو بأية وسيلة أخرى يختارها "(المادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية المعتمد بموجب قرار الجمعية العامة 2200ألف (د-21) المؤرخ 16 كانون الأول/ديسمبر 1966).

[2] Jean-Marie Auby. Robert Ducos-Ader, « Droit de l’information », D., 1982.

[3] Jean-Pierre Gridel, Alain Lacabarats, « Droit à la vie privée et liberté d'expression: fond du droit et action en justice », Gaz. Pal., 17/19 nov. 2002, n°321 à 323, Doct., p. 3-15.

لقد تطور الحق في حرية الاعلام بشكل كبير منذ الإعلان عنه. و قد وضعت الأسس الدولية لهذه الحرية من طرف الأمم المتحدة في الدورة الأولى للجمعية العامة في عام 1946. تم الاعتراف بحرية الاعلام بأنها "حق أساسي للإنسان وهي محك الاختبار لكل الحريات التي كرستها الأمم المتحدة"[1]. في الواقع فإن المقاربات غير متجانسة في تحديد مفهوم حرية الاعلام. في الولايات المتحدة، فإن القوانين المتعلقة بهذا المجال موجودة منذ ستينات القرن العشرين و تطبق على الولايات الخمسين وعلى الحكومة الاتحادية[2]. في كثير من الأحيان تم تفسير البند الأول من الدستور الأمريكي ليكون الحق في الاعلام الذي يتطرق إليه مبررا لصالح الصحافة في "الحق في المعلومة" من أجل إعطائها (و لباقي وسائل الإعلام الأخرى) حرية الوصول إلى الملفات التي تحوزها الإدارة و الحكومة[3].

في 2011 اعتمدت لجنة الأمم المتحدة لحقوق الإنسان تعليقا عاما على تفسير المادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية (المتعلقة بحرية الرأي وحرية التعبير). هذا التعليق الذي طال انتظاره منذ سنوات يقدّم توضيحات هامة. حيث تم تكريس فقرتين للحق في الحصول على المعلومة: الفقرة 18 دولة تنص صراحة على أن المادة 19(2) تتضمن الحق في الوصول إلى المعلومة

---

[1] قرار الأمم المتحدة رقم 59 (I) الصادر في 14 ديسمبر 1946، نص القرار متوفر على: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/033/10/IMG/NR003310.pdf?OpenElement

[2] القانون المتعلق بحرية الإعلام. (Freedom of Information Act) أنظر الدراسة المقارنة المتعلقة بحرية الاعلام في عدد من الولايات الأمريكية : Roger A. Nowadzky, « A Comparative Analysis of Public Records Statutes », 28 The Urban Lawyer, 65 (1996).

[3] Jean-Pierre Chamoux, « Données publiques. Un patrimoine commun ? », Les Cahiers du numérique 2013/1 (Vol. 9), p. 153-171

التي تحوزها السلطات العامة، والذي يتضمن "الملفات التي تحتفظ بها هيئة عامة، بغض النظر عن طريقة التخزين، ومصدر وتاريخ الإصدار". و تحدد الفقرة 19 قائمة من التدابير الرئيسية التي يتعين على الدول الأطراف إتخاذها لجعل هذا الحق فعّال[1].

وفي الوقت نفسه تطور هذا المصطلح في التشريعات الوطنية، من "حرية الاعلام" إلى "الحرية في الاعلام". يقترح كاتب كندي تعريفا لها كما يلي: " إن الحق في الاعلام هو حق طبيعي وأساسي للفرد والمجتمع في معرفة المعلومة وتعريف الآخرين بما يحدث، والذي من مصلحتنا أن نعرفه. حرية الاعلام هي حق طبيعي وأساسي للفرد و المجتمع في البحث عن المعلومة ومعرفتها وتعريف الآخرين بما يحدث، والذي من مصلحتنا أن نعرفه "[2]. وهكذا فإن مفهوم "المصلحة في المعرفة" هي في جوهر كل من الحق في الاعلام وحرية الإعلام. في الواقع فإن إضفاء الطابع الدستوري على حرية الصحافة يُعزّز الحماية الدستورية الممنوحة للاعلام. ويستفيد من حرية الاعلام سواء أولئك الناشرين أو المخاطبين، هذه الميزة لصيقة بالحق في إعلام الجمهور. و هو حق الجمهور في معرفة الحقيقة أو على الأقل المساهمة في ذلك. والواقع أن المواطن هو صانع القرار السيادي بسبب ورقة تصويته، لن يكون قادرا على استعمالها بشكل صحيح إذا لم يكن لديه معلومات كافية. إنه الظلم بعينه إذا كنا أمام نفس المعلومة ولكن ليست في متناول الجميع.

---

[1] Observation générale n° 34, Comité des droits de l'Homme, juillet 2011, CCPR/C/GC/34. http://www2.ohchr.
org/english/bodies/hrc/docs/gc34.pdf.

[2] Claude Jean Devirieux, «Manifeste pour le droit à l information, de la manipulation à la législation». Presse de l'Université du Québec. Québec. Canada (1 ère édition 2009).

خطر حجب المعلومة هو فرضية حقيقية، يمكن للحكومات استخدام الامكانيات المتاحة لها قانونا، بما في ذلك الاتفاقات الدولية، للحد من الوصول إلى المعلومة الكاملة[1]. هذه المشكلة لا تميّز الاتصالات الإلكترونية أكثر مما هو عليه الأمر في البيئة التقليدية، ولكنها مهمة جدا في العالم الرقمي الذي ينتظر فيه المستخدمون بصفة خاصة الولوج الشامل و الفوري لجميع البيانات الممكنة. ولكن أسس التقييد الذي يمكن للحكومة أن تفرضه على الحصول على المعلومة الكاملة وعلى وجه الخصوص ذات الصلة بضرورة الحفاظ على أمن الدولة وحماية الخصوصية وعدم الكشف عن هوية الأفراد[2]. غالبا ما يُسلّط الضوء في الحالة الأولى على قوانين مكافحة الارهاب التي يتم طرحها لتجنب الكشف عن بعض المعلومات[3] . هذه القوانين مع بعض الفروق تزيد من صلاحيات السلطات الحكومية (الشرطة والجيش والعدالة)، و تقيّد إِلَى حَدٍّ بَعِيد وفي كثير من الأحيان

---

[1] BLANTON T.S., National security and open government in the United States: Beyond the balancing test, in. National security and open government: striking the right balance. The Maxwell School of Syracuse University: New York, 2003 ; Mendel, T. (2003b). National security vs. openness: an overview and status report on the Johannesburg principles. National security and open government: striking the right balance. New York, The Maxwell School of Syracuse University.

[2] ومن الأمثلة على ذلك موقف الولايات المتحدة التي رفضت الكشف عن أسماء سجناء غوانتانامو، مدعية بحقهم في حرمة الحياة الخاصة ويتم بذلك انتهاك اتفاقيات جنيف. ومنذ ذلك الحين، صدر الحكم بإلزام السلطات بالإفصاح عن جميع المعلومات، أنظر:

Commentary (2005). "Delicious rulings form the Big Apple." The News Media & the Law 29(4).

[3] أمثلة عن هذه القوانين:

USA PATRIOT Act في الولايات المتحدة الأمريكية.

L.C. 2001, ch. 41 في كندا.

Anti-terrorism crime and security act de 2001 في بريطانيا، إلخ.

وصول المواطنين إلى معلومات معينة. و من الواضح أن هذه السياسة تتعارض مع حرية الوصول إلى المعلومة. في ظل الديمقراطية تستمد الحكومات شرعيتها وسلطتها من إرادة الشعب صاحب السيادة، وأنها يجب أن تخضع للمساءلة عن أفعالها من طرفه (« *accountability*[1] »).ونتيجة لذلك فإن الموظفين العموميين ليسوا مالكين للوثائق أو المعلومات التي يحوزونها بحكم وظائفهم، وللمواطنين الحق في الحصول عليها و طلب إبلاغهم بها. هذا هو المبدأ الأساسي للـــ " الحكومة المفتوحة " أو " الحكومة الشفافة " لترجمة المفهوم الأنجلوسكسوني « *Open Government* ».

هذا المفهوم أوسع في بريطانيا ويشمل حرية الوصول إلى المعلومات، ولكن لا يقتصر عليها: إنه يشمل أيضا شفافية الميزانية، ونشر الذمة المالية للمنتخبين ومسؤولي الحكومة، ومشاركة المواطنين.

إن اتفاقية مجلس أوروبا بشأن الوصول إلى الوثائق العامة في سنة 2009[2]، تدخل في إطار حركة التحرير العامة، وأتت لوضع اللمسات الأخيرة عليها. ووضعت مجموعة من المعايير الدنيا وتسعى إلى تشجيع الدول الأعضاء التي لم تتفاعل لجعل تشريعاتها متماشية مع هذه المعايير. في نفس الاتجاه أقرّت محكمة الدول الأمريكية لحقوق الإنسان من جهتها و لأول مرة في سنة 2006 بأن الوصول إلى المعلومة هو حق أساسي من حقوق الإنسان[3].

---

[1] المحاسبة.

[2] Convention du Conseil de l'Europe sur l'accès aux documents publics. Référence, STCE n°205. Ouverture du traité, Tromsø, 18/06/2009.

[3] CIDH, Caso Claude Reyes y otros c/ Chile, 19 sept. 2006, adresse: http://www.corteidh.or.cr/ casos.cfm?idCaso=245.

ورأت المحكمة أن المادة 13 المتعلقة بحرية الفكر والتعبير تتضمن حق ضمني في الحصول على المعلومات التي تحتفظ بها الإدارة وأنه ينبغي للدول أن تعتمد تدابير تشريعية. لجعلها فعال.

من أجل إعادة تموقع حرية الاعلام في سياق رقمنة البيانات، وإذا تمسكنا بالمطلب الأولي المتمثل في نشر المعلومات التي تحوزها الهيئات العامة، كان لابد من من إعادة نشر البيانات العامة في شكل رقمي. توسع الإنترنت وتعميمها زاد الطلب على المعلومة من الجمهور والشركات والمنظمات غير الحكومية. تدفق المعلومات ليس له حدود والمواطنون المعتادون على الوصول إل مصادر أجنبية للمعلومة على الأنترنت يريدون الحصول عليها من حكوماتهم. و إن التنظيم السلمي التقليدي للادارة، المبني على أساس احتكار المعلومة في أعلى الهرم الاداري، يفترض أن يتم إعادة النظر فيه لأنه لم يعد يلبي تطلعات المجتمع[1]. أكدت النصوص المعتمدة في نهاية القمة العالمية في جنيف (2003) وتونس (2005) بشأن مجتمع المعلومات أن وصول الجميع إلى المعلومة هو أحد الدعائم الأساسية لمجتمعات المعرفة الشاملة، كما أقرت بإمكانات تكنولوجيا الاعلام والاتصال، شريطة أن تكون في متناول الجميع، لتسهيل إكتمال الحق في المعلومة للجميع[2].

كما ينبغي أن يكون مفهوما اليوم أن الانفتاح على الجمهور يعني خاصة إزالة العقبات التي تعترض حرية استغلال وإستنساخ البيانات. فتح وإعادة استخدام كل هذه البيانات يفتح آفاق اقتصادية و تجارية جد واعدة لأنه يسمح بتطوير تطبيقات وخدمات مبتكرة، وتحفّز على النمو.

وقد أدركت الحكومات إمكانات مخزون البيانات الرقمية التي لديها على المستوى الوطني والمحلي. وبالتالي سيتم نشر هذه البيانات الرقمية العامة أو

---

[1] Perrine Canavaggio, « Vers un droit d'accès à l'information publique », Les avancées récentes de normes et des pratiques, UNESCO, 2013, p. 17, adresse: http://unesdoc.unesco.org/images/0022/002268/226875f.pdf.

[2] إعلان مبادئ وخطة عمل جنيف وجدول أعمال تونس لمجتمع المعلومات على الموقع: http://www.itu.int/wsis/index-fr.html

الخاصة، والصادرة عن جماعة محلية أو مرفق العام على أساس رخصة مفتوحة دون تقييد تقني أو قانوني أو مالي في إطار إجراء منصة البيانات المفتوحة « *Open Data* »[1]. وكانت الولايات المتحدة وبريطانيا أول من فتح الوصول إلى البيانات العامة على بوابات data.gov في ماي 2009 وجانفي 2010، و تتزايد في العالم الآن المبادرات الحكومية في هذا المجال. بتاريخ 18 جوان 2013 وقّع رؤساء مجموعة الدول الثماني (G8) ميثاقا لفتح البيانات العامة الذي يؤسس لمبدأ الفتح المفترض لهذه البيانات ؛ و بتأكيده على مبدأ مجانية الاستخدام وتركيزه على المعايير المفتوحة، فإنه يعزز وصول الجميع إل المعلومة ويُشجع الابتكار[2].

---

[1] تم تدريجيا تقنين حركة البيانات المفتوحة من وجهة نظر قانونية في البلدان الديمقراطية، وكان ذلك بظغط مارسته فرق عمل تتألف من خبراء عن المجتمع المدني أو منظمات غير حكومية. أنظر:

B. Jean, « De l'Open source à l'Open data », Interopérabilité & GéoInformation, 29 nov. 2011, adresse: http://georezo.net/blog/geointerop/2011/11/29/de-l-open-source-a-l-open-data / ; Marchand, Jennifer L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique ? In: La semaine juridique. Administrations et collectivités territoriales n° 7, 2014, 17 février p. 25-31 ; Eléonore Varet, « L'Open Data. Point de rencontre entre le libre et les données publiques », Expertises, n° 371, juill. 2012, p. 254-257.

واليوم تخضع البيانات المفتوحة لتنظيم قانوني على الصعيد الأوروبي، أنظر:

Guy Lambot, Réutilisation des informations du secteur public: la révision de la directive 2003/98/CE est en marche, Légipresse septembre 2012, n°297, p. 517-522 ; Guy Lambot, «Réutilisation des informations du secteur public: entrée en vigueur de la directive 2003/98/CE révisée". LEGIPRESSE. septembre 2013, p. 500-507.

[2] أنظر: http://fr.scribd.com/doc/148580461/Charte-du-G8-pour-l-Ouverture-des-Donnees-Publiques-Francais

وقد التزمت كل دولة على وضع خطة عمل بحلول نهاية سنة 2013، تهدف إلى إحترام مبادئ الميثاق من خلال تطبيق أفضل الممارسات والالتزامات الجماعية المفصلة في الملحق التقني إلى غاية نهاية سنة 2015. ولكن من الضروري أيضا أن تتطور منصة البيانات المفتوحة في ظل احترام الحقوق والحريات العامة الأخرى، بما في ذلك الحق في الخصوصية، والحق في الوصول الشخصي إلى البيانات، والحق في وصول الجمهور إلى المعلومة. لقد تم في الولايات المتحدة الأمريكية تحديد عدة عوامل هامة خلال وضع السياسات الخاصة بحماية الخصوصية في سياق الوصول إلى قواعد البيانات العامة[1]. ويتعلق الأمر خاصة باحترام البند الأول من الدستور، واحترام حرية الاعلام، والمصلحة الاجتماعية المتمثلة في كلفة تطبيق القانون[2].

كما تم وضع ثلاثة معايير لحماية الحياة الخاصة في سياق الحق في الوصول إلى البيانات الموجودة في قواعد البيانات: الحفاظ على البيانات الكافية والكاملة والمحدثة و التي يمكن أن تخضع للمراجعة. معرفة المواطنين للاستخدامات التي يمكن إزالتها. واستخدام البيانات من قبل المنظمات يستند فقط على مبدأ " بحاجة إلى معرفة " بناء على المهام التي كلفوا بها.

في حين منذ أواخر القرن العشرين كان ينظر إلى حرية الإعلام كإصلاح للحكم الإداري في المقام الأول، بمعنى أنه كان للأفراد الحق في الوصول إلى المعلومات التي تحتفظ بها الهيئات العامة و العدالة[3]، واليوم يضاف إلى ذلك مفهومها الجديد الذي ينطوي على حق أساسي من حقوق الإنسان[1].

---

[1] The Privacy Protection Study Commission (PPSC).

[2] Sitkin, Irwin J., « Comment on 'Privacy Cost Research: An Agenda' », dans «Computers and Privacy in the Next Decade», p. 61-64.

[3] ويشمل هذا الجانب من حرية المعلومات حرية وصول المواطنين إلى الحق في الحصول على المعلومات القانونية. وفي هذا السياق، فإن سياسات النشر الحر للقانون تجد مصادرها في

يعتبر منظرو علم التحكم الآلي مثل نوربرت وينر، أن هناك صلة أساسية بين حرية الاعلام في مفهومها التقني وحرية الإنسان بالمعنى السياسي[2]. من أجل ضمان هذه الأخيرة، لا بد من أن تتدفق المعلومات بحرية[3]. تم دعم حرية التدفق في أواخر 1950 من قبل ما يسمى بـــ « *academic hackers* » أو الهاكر الأخلاقي، ويتمثل خطاب هواة برمجة الكمبيوتر في أن الانفتاح و المشاركة ورفض السلطة وضرورة العمل الشخصي هي طرق لتغيير العالم. فكرة أن " كل معلومة يجب أن تكون حرة " هو أصل فلسفتهم التي أعادوا بها النظر في العلاقة بين الانسان و جهاز الكمبيوتر عن طريق فعل كل شيء من أجل أن يكون هذا الجهاز موجودا في خدمة للفرد بدلا من أن يكون وسيلة تحكم في هذا الأخير[4].

أصبحت الانترنت على حد السواء وسيلة للاتصال الشخصي مثل الهاتف، ووسيلة إعلام شاملة مثل الراديو أو التلفزيون. وهي تعمل إذا على التقارب بين هذين البعدين، بشكل يمكن فيه لمعلومة صادرة عن وسائل الإعلام الكبرى أن

التشريعات الأمريكية حيث هناك عرف قديم في التخلي عن أي حق للمؤلف على النصوص القانونية، فضلا عن التطور المبكر للإنترنت، أدت إلى تنفيذ مبادرات مثل مشروع HERMESالذي بدأ في 11 ماي ١٩٩٠، والذي أتاح الوصول الحر إلى نصوص قرارات المحكمة العليا الأمريكية في شكل إلكتروني. هناك اليوم مئات من المواقع التي تقدم مجموعات مختلفة في التشريع، الاجتهاد أو الفقه في الولايات المتحدة الأمريكية.

[1] Tony Mendel « Liberté de l'information Étude juridique comparative » (Unesco. 2ème édition. 2008) adresse: http://portal.unesco.org/ci/en/files/26159/12284883325freedom_information_fr.pdf/freedom_information_fr.pdf.

[2] Norbert WIENER, « Cybernétique et Société. L'usage humain des êtres humains », Paris, Union générale d'éditions, 1971 [1950].

[3] Ronan Le Roux, « L'homéostasie sociale selon Norbert Wiener », Revue d'histoire des sciences humaines, n° 16, 2007, p. 113-135.

[4] Steven Levy, « L'Ethique des hackers », Paris, Globe, 2013.

تتداولها الشبكات الشخصية، وعلى العكس فالمعلومة الصادرة عن الشبكات الشخصية يمكن أن تسلك طريقها نحو وسائل الإعلام الكبرى[1].

وعلاوة على ذلك فإن الحاجة للتعاون الدولي أصبحت من البداهة بمكان، لضمان احترام حرية التعبير وكذا حرية الاعلام في السياق الرقمي. حيث تم الاعتراف بهذه الأخيرة رسميا على المستوى الدولي. على سبيل المثال وفي بيانهم الصادر بتاريخ 13 ديسمبر 2011، خرجت الدول الأعضاء في منظمة التعاون الاقتصادي و التنمية (OCDE) بالتالي: "إن اقتصاد الإنترنت مثل قدرة الأفراد على التعلم وتبادل المعلومات و المعرفة، والتعبير والاجتماع و تكوين الجمعيات، والتي تعتمد على التدفق العالمي الحر للمعلومات. لتسهيل التدفق الحر للمعلومات على شبكة الإنترنت، من المهم أن نعمل معا لتحسين التوافق في ميدان المبادلات التجارية على المستوى العالمي على الرغم من تنوع القوانين و الأنظمة"[2].

في هذا السياق، فإن المجتمع المدني، و المنظمات غير الحكومية و الصحفيين يلعبون دورا رئيسيا في إحترام معايير الكشف الأقصى للمعلومات.

كانت منظمة Open Society Justice Initiative أول من نشر سنة 2006 دراسة تجريبية للقوانين و ممارسات الوصول إلى المعلومة في 14 دولة. في الواقع freedominfo.org هي بوابة مركزية تربط إفتراضيا المدافعين عن

---

[1] Benjamin Loveluck, « Permanence et recomposition du partage public/privé à l'ère d'Internet: le personnel et le politique à l'épreuve de la libre cicrulation de l'information », Congrès AFSP Paris 2013, sect. Thématique 66, « Le partage publicprivé: généalogie et recomosition », adresse: http://www.congres afsp.fr/st/st66/st66loveluck.pdf.

[2] OCDE, « Recommandation du Conseil sur les principes pour l'élaboration des politiques de l'Internet », C(2011)154, 13 déc. 2011.

الوصول إلى المعلومة في العالم منذ عام 2002. ويقدم معلومات كاملة عن حالة الحق في الوصول إلى المعلومة في العالم. Freedom of Information Advocates Network (Foianet) و The Acces Initiative مثال لشبكتين دوليتين تهدفان إلى تسهيل التعاون و تطوير مشاريع مشتركة لحرية الوصول إلى المعلومة.

ممارسة الحريات العامة في الواقع الرقمي.

مفهوم عالمية الإنترنت يسلط الضوء على الترابط بين المكونات المعيارية والفنية والاجتماعية، الخ. لهذا النظام البيئي المنفتح و الفريد من نوعه. وفي هذا السياق يمكن أن يساعد أيضا على التركيز على التناغم المستمر بين النمو واستخدام الإنترنت وحقوق الإنسان. في الواقع ونظرا للتكامل القوي مع الحق في حرية التعبير وحرية تدفق المعلومة، يمكن أن تفهم عالمية الإنترنت على أنها وسيلة أساسية لتحقيق مجتمع المعلومات ، أيضا وبالمساهمة في النقاش العام عبر الإنترنت، يشارك الأفراد في الواقع في المجتمع المدني، ببناء سلطة مضادة للحكم. بفضل مواقع الويب والشبكات الاجتماعية، ومنتديات المناقشة أو المدونات، ومستخدمي الإنترنت لديهم الفرصة لممارسة حريتهم في التجمع و تكوين الجمعيات على مستوى جديد كليا .

الحق في الوصول إلى الأنترنت.

إنترنت عالمية هي إنترنت حرة، قائمة على الحقوق، مفتوحة ومتاحة. كما تشرحها وتعمل على ممارستها على سبيل المثال منظمة اليونسكو[1]، ومبدأ العالمية

---

[1] UNESCO/WSIS, D. Frau-Meigs, « Exploring the evolving mediascape: towards updating strategies to face challenges and seize opportunities? », 2013, adresse:

يتضمن عدة أنواع من الضمانات. و يتعلق الأمر على وجه الخصوص، بالوصول الشامل للإنترنت، والهواتف المحمولة وتكنولوجيا المعلومات والاتصالات، الخ. لضمان هذا الوصول الشامل، ينبغي الاشارة إلى أربعة بديهيات أساسية مترابطة والتي توجد في أصل وجود شبكة الإنترنت، و هي: أن الإنترنت يقوم على حقوق الإنسان (الإنترنت الحرة)، وأنها مفتوحة وفي متناول الجميع، وأخيرا أنه يتم تزويد الإنترنت من خلال مشاركة عدة فاعلين. إن تطبيق هذه المعايير الأربعة يعمل على خلق بيئة يكون فيها كل المستخدمون سواسية في الوصول إلى المعلومة ويتم معالجة جميع المعلومات على قدم المساواة في عملية نشرها للجمهور.

والهدف إذن هو إقامة نظام يكون فيه الوصول إلى الشبكة مبنيا على مبدأ عدم التمييز والذي يكون فيه فائدة للأفراد وكذا المحتوى. وعلى نحو أكثر تحديدا، يجب أن يضمن كل مستخدم الوصول إلى وسائل الاتصال الإلكترونية، وأن يتم نشر كل محتوى عن طريق الوسائل ذاتها.

إن الوصول إلى الإنترت هو مفهوم متعدد الأبعاد يشمل الوصول المادي ليس فقط على شبكة الانترنت ولكن أيضا الوصول باللغة المحلية الخاصة بالمستخدم، والوصول لذوي الاحتياجات الخاصة والوصول إلى المحتوى الرقمي المنتج محليا (أولا). علاوة على ذلك فإن هذا الحق في الوصول إليها يخضع لاحترام مبدأ الحياد التكنولوجي (ثانيا). القواعد المعتمدة لحماية الوصول إلى البنية التحتية يجب أن تكون عامة بما فيه الكفاية ليتم تطبيقها على كل اتصال، دون الأخذ بعين الاعتبار نوع الجهاز أو التكنولوجيا المستخدمة. لهذه المسألة أهمية خاصة، حيث

---

http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/exploring_the_evolving_mediascape_Report_final_version_DFM.pdf.

أن الضمانات المقدمة للاتصال بالشبكة يتجاوزها الزمن بسرعة، مع تطور وتعدد الأدوات الرقمية المختلفة، مثل أجهزة الكمبيوتر، والهواتف واللوحات الذكية، وأجهزة التلفاز، إلخ.

أولا: الحق في الاتصال بالإنترنت: حق أساسي جديد؟

الهيئة القضائية الأولى التي تطرقت إلى مسألة الرهانات التي يطرحها الوصول إلى الإنترنت بالنسبة لحرية التعبير، كانت المحكمة العليا في الولايات المتحدة الأمريكية في سنة 1997[1].

وقد أقرّت لجنة الأمم المتحدة لحقوق الإنسان في 2011 أن تطوير "تكنولوجيا الاعلام والاتصال مثل الإنترنت ونظم النشر الالكتروني للمعلومة باستخدام التكنولوجيا المتنقلة قد حولت ممارسات الاتصال في العالم "، ودعت الدول إلى " اتخاذ جميع التدابير المناسبة لتشجيع استقلال هذه الوسائل الجديدة وضمان توصّل الأفراد إليها "[2]. وفي وقت لاحق، في ماي 2011 تم تفسير التقارير المقدمة من طرف مقرر الأمم المتحدة الخاص حول حرية التعبير والرأي Frank de la Rue من قبل الكثير من الفقه بمثابة إعلان حق الوصول إلى الإنترنت كحق من حقوق الإنسان[3].

---

[1] قرار المحكمة العليا الأمريكية :
Reno, Attorney General of the United States et al. c/ American Civil Liberties Union et al., n° 96-511, 26 juin 1997.

[2] Comité des droits de l'homme. 102e session. Genève, 11-29 juillet 2011. Observation générale no 34. Article 19.

[3] Andris Mellakauls, « L'accès à Internet – un droit de l'homme? », Cons. E., CDMSI(2012)Misc3, 27 févr. 2012.

في شهر جويلية من نفس العام، أعلنت ممثلة "من أجل حرية وسائل الاعلام" في منظمة الأمن والتعاون في أوروبا (OSCE) في تدخلها أمام لجنة هلسنكي للولايات المتحدة أنه " من أجل الاشادة بالمساهمة الفريدة للإنترنت في الديمقراطية التشاركية، وحرية التعبير وحرية وسائل الإعلام، فإنه كان من المناسب تكريس الحق في الوصول إلى الإنترنت في المستوى الذي يرقى إليه، كحق من حقوق الإنسان ذو مرتبة دستورية "[1].

في الواقع أصبحت الشبكة الالكترونية الآن أداة أساسية لتطوير النشاط الاقتصادي، أو فكرة سياسية أو اتصال اجتماعي. بالفعل فإنه لم يعد من الممكن التفكير في تطوير المجتمع و الفرد "المعزول" عن الموارد الرقمية[2].

و أمام هذه الحقائق فإن العديد من الدول الأعضاء في الاتحاد الأوروبي تعتبر الإنترنت كحق أساسي.

وهكذا اعتمدت دولة إستونيا قانونا للاتصالات في سنة 2001، أضافت المادة 5 منه الدخول إلى شبكة الإنترنت إلى قائمة المواد التي تدخل في التزامات الخدمة الشاملة للمتعاملين. قامت اليونان بدورها بتكريس حق الوصول إلى الإنترنت في عام 2001[3] بإضافة المادة a5 إلى الدستور، التي تنص في الفقرة 2 على أنه لكل شخص الحق في المشاركة في مجتمع المعلومات. و يضيف

---

[1] دعت ممثلة منظمة الأمن والتعاون في أوروبا لحرية الإعلام، د. مياتوفيتش، الحكومات إلى الاعتراف بحق الوصول إلى الإنترنت كحق من حقوق الإنسان. بيان صحفي لمنظمة الأمن والتعاون في أوروبا، 16 جويلية http://www.osce.org/fom/810062011.

[2] Laure Marino, « Le Droit d'Accès à Internet, Nouveau Droit Fondamental », D., n° 30, 2009, n° 2045. Nicola Lucchi, « Can the Internet be a Human Right ? », Human Rights and Human welfare, n° 01/2004 ».

[3] دستور اليونان (التعديل السابع الصادر في 6 أبريل 2001).

النص أن تسهيل الوصول إلى المعلومة المنشورة إلكترونيا، فضلا عن إصدارها وتبادلها ونشرها من واجبات الدولة[1].

في أكتوبر 2009 عدّل المشرع الفنلندي القانون المنظم لسوق الاتصالات[2] وأدرج الحق في الوصول إلى الإنترنت مع سرعة لا تقل عن 1 ميجابايت في الثانية. بهذه الطريقة و للمرة الأولى تم الاعتراف بالتدفق العالي بوصفه حقا شاملا يكفله نص تشريعي. بينما دخل التعديل حيز النفاذ في 1 جويلية 2010، كان من المقرر أصلا أن الحد الأدنى للتدفق المضمون ينتقل إلى 100 ميغابايت في الثانية قبل نهاية عام 2015[3]. وعلاوة على ذلك فإن الاتصال ذو التدفق العالي بسرعة 1 ميغا بايت في الثانية مكفول أيضا من قبل التشريع الإسباني منذ اعتماد قانون الاقتصاد المستدام في 4 مارس2011[4].

من جهة الاجتهاد القضائي قضت المحكمة الدستورية (SalaConstitucional) كوستاريكا في حكمها الصادر في 30 جويلية 2010 أن التأخير الذي تسببه الحكومة في تحرير سوق الاتصالات يعتبر بمثابة انتهاك

---

[1] تنص المادة 5 ف2 من الدستور اليوناني:

« All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19 ». Adresse:
http://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf.

[2] أنظر المادة 60 من القانون الفنلندي المنظم لسوق الاتصالات والمرسوم التنفيذي 2009/732 المتعلق بالحد الأدنى لسرعة تدفق الانترنت.

[3] تقرير الاتحاد الدولي للاتصالات (UIT) أنظر الموقع:
http://www.itu.int/net/itunews/issues/2010/06/pdf/201006_34.pdf

[4] أنظر المادة 52 من قانون الاقتصاد المستدام الاسباني والمرسوم التنفيذي رقم 2011/726.

للحريات الأساسية. من ناحية أخرى، في إيطاليا ومنذ 2010 دار نقاش حول ضرورة إدماج الحق في الوصول إلى الإنترنت في الدستور، تقرر أخيرا أن الصياغة الحالية للمادة 21 بشأن حرية التعبير كافية لحماية هذا الحق، من دون الحاجة إلى ذكره مباشرة وبالتالي تغيير النص الدستوري[1].

نجد مثالا عمليا لهذا التفسير في فرنسا حيث أدرك المجلس الدستوري الاهتمام المتزايد الذي يشكله الوصول إلى الشبكة الرقمية بالنسبة للشركات والأفراد، وقرّر تكريس الطابع الأساسي لهذا الحق في الوصول إلى وسائل الاتصال الإلكترونية. هذا الضمان غير المباشر جاء بعد التفسير التدريجي لحرية الاعلام عن أفكاره وآرائه، حيث يعترف القاضي الدستوري بهذا الحق في الوصول إلى الإنترنت كنتيجة ضرورية للحق الأساسي في حرية التعبير. ولذلك حتى وإن اعتبر تابعا لحرية التعبير والإعلام، وليس حقا في الوصول إلى الإنترنت بالمعنى الدقيق للكلمة، فإنه يبقى رغم ذلك محميا. كل ما سبق يستنتج من قرار 10 جوان2009[2]، حيث نظر القاضي الدستوري في الطعن ضد قانون Hadopi[3] و أعلن أن "حرية الاتصال و التعبير، المنصوص عليها في المادة 11 من إعلان حقوق الإنسان والمواطن لسنة 1789، تخضع لحماية الاجتهاد المستقر للمجلس الدستوري (...).

بالنظر إلى ما وصلت إليه وسائل الاتصال اليوم والتطور العام لخدمات الاتصال العامة عبر الإنترنت فضلا عن الأهمية التي توليها هذه الخدمات

---

[1] بالفعل تنص المادة 21 من الدستور الايطالي على أنه " للجميع حق ابداء الرأي بحرية قولا وكتابة وبأي من وسائل النشر الأخرى.

[2] Cons. const., déc. n° 2009-580 DC, préc. c/ n°33.

[3] Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet (1), JO n° 135 du 13 juin 2009, p. 9666, texte n° 2.

للمشاركة في الحياة الديمقراطية والتعبير عن الأفكار والآراء فإن هذا الحق يشمل حرية الوصول إلى هذه الخدمات [خدمات الاتصال العامة عبر الإنترنت] ".[1]

يؤكد المعلقون على هذا القرار على أنه لإيجاد رابط بين حرية منصوص عليها في أواخر القرن الثامن عشر و السياق الحالي، يعتمد المجلس الدستوري على حالة التكنولوجيا والسوق(حصة كل وسيلة من وسائل الاتصال المختلفة)، و على الممارسة الاجتماعية الحالية التي تكرس الاستخدام الواسع النطاق للإنترنت من قبل الجمهور، وأخيرا على الدور الذي تحتله وسائل الاتصال الجديدة في الحياة الديمقراطية و النقاش العام.

و من المفارقات أنه في حين أن الحق في الوصول إلى الإنترنت الذي يتضمن الحق في الوصول إلى المعلومة الرقمية والحق في نشر المحتوى الرقمي، يظهر بشكل متزايد كمكتسب في مجتمع المعلومات وأن مكافحة الفجوة الرقمية و الرقابة على المحتوى مستمرة، هناك أحداث معيّنة تطرح إشكالية

---

[1] Comm. de la décision n°2009-580 DC du 10 juin 2009, Cah. Cons. Const., n°27, janv. 2010. V. égal. Laurence TELLIER-LONIEWSKI, Anne PLATON, Alain Bensoussan, « Loi « création et Internet »: le feuilleton législatif continue... suite et fin ? », Gaz. Pal., n° 203-204, 22 et 23 juill. 2009, p. 3-6 ; Jean-Michel Bruguière, « Loi « sur la protection de la création sur Internet »: mais à quoi joue le Conseil constitutionnel ? », D. n° 26, 2009, p. 1770-1771 ; Florence Chaltiel, « La loi Hadopi devant le Conseil constitutionnel » LPA, n° 125, 24 juin 2009, p. 7-11 ; David El Sayegh, « Le Conseil constitutionnel et la loi Création et Internet: une décision en trompe-l'oeil », Lég., n° 263, 2009, p. 97-98 ; Jean-Philippe Feldman, « Le Conseil constitutionnel, la loi « Hadopi » et la présomption d'innocence », JCP G, n° 28, 2009, p. 25-28 ; Michel Verpeaux, « La liberté de communication avant tout. La censure de la loi Hadopi 1 par le Conseil constitutionnel », JCP G, n° 39, 2009, p. 46-52.

جديدة تتعلق بـــ " الاستخدام المفرط للإنترنت "[1] أو حتى بـــ"الإدمان على الإنترنت"[2] أو "إدمان الإنترنت"[3]. يترتب عنها "الاجهاد الرقمي"[4] والذي يرتبط بصعوبات نفسية و جسدية، كنتيجة مباشرة للعزلة والانسحاب الاجتماعي. والواقع أنه بدأت النتائج المترتبة على الاستخدام المفرط للإنترنت في الظهور في كل مستويات الحياة، لدرجة أنه في حين أن بعض الدول – مثل كوريا الجنوبية – تنظر إليه على أنه مرض جديد، والبعض الآخر – مثل كاليفورنيا – تعمل على إنشاء مراكز علاجية من إدمان الانترنت، في مبادرة تعد الأولى وطنيا وعربيا تم إنشاء في الجزائر أول خلية لعلاج الإدمان على الإنترنت بالمؤسسة الاستشفائية للصحة الجوارية بشير منتوري بقسنطينة[5].

ثانيا: مبدأ حياد الإنترنت.

ويرتبط الحق في الوصول إلى الانترنت ارتباطا مباشرا بمبدأ الحياد. ويستند هذا المبدأ الذي تطرق إليه لأول مرة في عام 2003 الأستاذ T. Wu من جامعة كولومبيا في الولايات المتحدة الأمريكية، إلى الوصول الحر إلى شبكة الانترنت وفقا لعناصر ثلاثة: القابلية للتوصل والانفتاح والقابلية للتشغيل. فهو إذن مبدأ بعدم التمييز بحيث أن الشبكة المحايدة هي شبكة تنقل جميع البيانات دون أي تمييز أيا كان المحتوى والمصدر والمتلقي، دون أن يكون هناك امتياز لبروتوكول اتصال معين أو تعديل للمحتوى، وهذا بأقصى فعّالية ممكنة. وبهذا المعنى يشير

---

[1] « Ultraconnexion ».

[2] « Cyberdépendance ».

[3] « Cyberaddiction ».

[4] " Burn out".

[5] ع. بوشريف، "في مبادرة تعد الأولى وطنيا وعربيا. إنشاء أول خلية لعلاج الإدمان على الإنترنت والفايسبوك بالجزائر"، جريدة الشروق، 2016/05/24.

مبدأ الحياد إلى الفكرة الأولى في انشاء الإنترنت التي تستند إلى مبدأ "المجهود الأفضل" « *best effort* ».

وفي هذا الاتجاه فقد وضعت هيئة الظبط الأمريكية FCC قائمة أربع حريات يجب أن تحترم على شبكة الإنترنت في إطار المحافظة على حيادها. وفي قضية "نهر ماديسون" « *Madison River* »[1] أصدرت اللجنة الفدرالية مبادئ توجيهية، تم تجميعها لاحقا في بيان السياسة العامة، تنص على أنه يجب على كل مستخدم إنترنت أن يكون قادرا دائما على الوصول إلى أي محتوى قانوني يختاره، استخدام أي تطبيق أو خدمة قانونية، ربط أي جهاز بالشبكة لا يلحق بها ضررا، وأخيرا للاستفادة من اختيار أحد مقدمي الخدمات ومن المنافسة الفعالة بينهم.

بالفعل فإن الإنترنت المحايد هو واقع يشير إلى صورة للشبكة تحترم قدر الإمكان حقوق وحريات الفرد. من الناحية النظرية لكل شخص مكانه على قدم المساواة. ولا يوجد تمييز في التسهيلات المتاحة لمستخدمي الإنترنت من طرف مقدمي الخدمة: لا من حيث السعة التقنية للتخزين والنقل ولا سرعة الإرسال ولا تكلفة الخدمة. وبهذا المعنى فإن الإنترنت المحايد يقترب من فكرة الإنترنت الحر، وهو الهدف الذي يتقاسمه جزء كبير من المجتمع الرقمي. ومن خلال تطبيقه على الوسطاء ومقدمي الخدمات التقنية المرتبطين بشبكة الانترنت، يهدف مبدأ الحياد إلى ضمان احترام الحريات العامة لمستخدميه: حرية التعبير والاتصال، وحرية الاعلام، وحرية المعتقد، وحرية المبادرة والاختراع، إلخ.

---

[1] « In the Matter of Madison River Communications, LLC and affiliated companies ». Consent Decree DA 05-543.
FCC. 2005, adresse: https://apps.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf.

حرية التواصل على الأنترنت: عنصر أساسي في الديمقراطيات العصرية.

و بصرف النظر عن القضايا المتعلقة بالفجوة الرقمية و الرقابة على الاتصالات الإلكترونية المترتبة عن التدابير الادارية المقيّدة، فإن الإنترنت هي مكان عام للاجتماع وتبادل الأفكار، شامل إلى أبعد حد ممكن (أولا). حتى عندما تتعرض للقيود، إلا أنها تبقى تمثل قلب التعبير الديمقراطي، مما يجعلنا نفكر في أن المجتمع الرقمي قد يكون أفضل وسيلة لقيام الديمقراطية (ثانيا).

أولا: فضاء عام جديد لممارسة الديمقراطية المباشرة.

تشكل الإنترنت فضاءا عاما جديدا عابرا للأوطان والذي يكمّل الفضاءات التقليدية الوطنية المتصلة بالإذاعة والتلفزيون والكتب والصحف. ويتميز هذا الفضاء الجديد على وجه الخصوص بإنفصاله شبه الكامل عن الجغرافيا الاقليمية للدول[1]، كما تساهم أيضا في تشكيل جمهور عابر للأوطان يتواصل على نطاق عالمي.

بعد أن أدت إلى تغيير عميق للفضاء العام، فإن الإنترنت تعيد وصف المجال التقليدي الذي يعتبر المكان الخاص حيث تمارس المواطنة في الديمقراطيات الليبرالية. والواقع أن شكل الفضاء العام على الإنترنت يختلف عن المفهوم

---

[1] في هذا الاتجاه يعتقد ج. كان أنه:

« The ideal of a unified public sphere and its corresponding vision of a territorially bounded republic of citizens striving to live up to their definition of the public good are absolute. », v. J. Kaeane, « Structural transformations of the public sphere », The Communication review, vol. 1, n° 1, 1995, p. 8.

التقليدي للمصطلح متى لم يعد المكان الذي تمارس فيه السلطات العمومية صلاحياتها، فالفضاء العمومي كما كان يتصوره الفلاسفة هو وساطة بين المجتمع المدني من جهة و ممارسة السلطة العامة من جهة أخرى[1].

هذا الفضاء العام لم يعد المكان المخصص لممارسة سلطة الدولة باعتبارها تجسيدا للشأن العامة على حساب التبادلات الشخصية التي تقع داخل المجتمع المدني. أصبح لديه الآن قدرة جديدة على التنظيم الذاتي بـــ "جمهوره المشارك"[2].

في الواقع ونظرا لعدد مستخدمي الإنترنت المتزايد وكتلة البيانات المشتركة الهامة و المتنوعة على نحو متزايد، نشهد ظهور شكل جديد من أشكال "الديمقراطية المباشرة"[3] ألا وهو « self government »[4].

الجمهور الموجود على الإنترنت مماثل للنشطاء الذين يشاركون في الحياة السياسية بشكل آني. في هذا المعنى فإنه ليس الجمهور بالمعنى التقليدي للكلمة أي مجموعة سلبية من الأشخاص الذين تتفاعل بعد فوات الأوان، و الذي يتمثل دوره في مساندة أو انتقاد الحكام، ولكن جهاز كامل يتمثل دوره في مراقبة الهيمنة السياسية من خلال ضمان منع انتهاكات الحكومة. بفضل تكنولوجيا الاعلام

---

[1] أخذ يورغن هابرماس (Jürgen Habermas) مفهوم الفضاء العمومي (espace public) عن كانط E.Kant الذي قال به و تم استعماله بكثرة في مجال التحليل السياسي منذ سبعينيات القرن الماضي، فهو الفضاء الوسطي الذي تكوّن تاريخيا في زمن الأنوار بين المجتمع المدني و الدولة ، إنه أيضا المكان المتاح مبدئيا لجميع المواطنين حيث بإمكانهم الاجتماع لتكوين رأي عام

. Dominique Wolton, l'espace public, cahiers français, N° 218, Mai - Juin 1997, page 66

[2] Julien Levrel, « Wikipedia, un dispositif médiatique de publics participants », Réseaux, n° 138, 2006, p. 185-218.

[3] Lucien Sfez, « Internet et les ambassadeurs de la communication », Le monde diplomatique, mars 1999, p. 22-23.

[4] "الحكم الذاتي".

والاتصال لم تعد تقتصر المشاركة في الديمقراطية في مجرد عملية التصويت مرة واحدة بين الحين والآخر.

و لكن هي المشاركة الحقيقية، والمساهمة[1]. تؤدي الانترنت وظيفة التبليغ السريع بالسماح بتتبع مثلا المسائل التي تم تجاهلها أو تحويل معنى ما يعبر عنه في وسائل الإعلام. من خلالها يشارك المواطنون في النقاش العام وتفكير الحكومات بطرق مختلفة: كناخبين للتعبير عن آرائهم وإعطاء أصواتهم، كأعضاء في الهيئات التطوعية للدفاع عن حقوقهم و مصالحهم و في المجتمع العلمي لتقديم خبراتهم أو في المجتمع المدني للمساهمة في الاستشارات العامة.

لقد أصبح من المعمول به اليوم الاطلاع على برامج الأحزاب السياسية على مواقعها الرسمية، وخلق مدونات دعم المرشحين للانتخابات وتتبع منشورات السياسيين، خصوصا عبر الشبكات الاجتماعية مثل تويتر. المثال الأمريكي للحملة الانتخابية الرقمية " البيت الأبيض 2.0 " هو أيضا دليل على أن العالم الرقمي هو "العنصر الاستراتيجي للحملة"[2]. وبالنسبة للمرشحين السياسيين، فإن "حق المشاركة" الذي يوصف كحق أساسي جديد على شبكة الانترنت، مع كل المزايا التي يقدمها للمواطنين، يتحول تدريجيا إلى "واجب مشاركة" جديد للمترشحين السياسيين الذين يعتمد نجاحهم في الانتخابات إلى حد كبير على وجودهم و شعبيتهم على الإنترنت.

من ناحية أخرى لا ينبغي مع ذلك تجاهل الجوانب السلبية للديمقراطية الإلكترونية. في الواقع وبتجاوز التضامن المحلي بسبب تكنولوجيا المعلومات

---

[1] Béatrice Vacher, « Communication et débat public: les réseaux numériques au service de la démocratie », Paris, l'Harmattan, 2013.

[2] Chantal Enguehard, « Internet. Avec Obama, bienvenue à la Maison Blanche 2.0 », Jus Politicum, Revue de droit politique et de droit constitutionnel, n° 2, janv. 2009, p. 93.

والاتصال التي قد تضعفه، وعندما لا يكون هناك بديل حقيقي. و متى كان استخدام الاتصالات الإلكترونية في الأساس ممارسة الفردية، فإنه يمكن أن يضاعف تحلل الارتباط الاجتماعي والذي يؤدي إلى تراجع قيم المواطنة كعريضة المساندة الرقمية ذو الفعّالية الجد ضعيفة في كثير من الأحيان والتي تكون على حساب أشكال التعبير التي هي في تراجع، مثل المظاهرات والاجتماعات والمناقشات العامة[1]. ولذلك فإن ولادة الديمقراطية الإلكترونية لا تعني إكتمالها وعليها مواجهة عددا من الصعوبات الاجتماعية والفنية والقانونية، كعدم القدرة على دعم المشاركة في مبادرات جديدة، والحاجة إلى تعزيز وثوقية الخدمات (لا سيما في التصويت الإلكتروني وأخطار انتحال الهوية) أو حتى ظاهرة المعلومات الزائدة عن الحد[2].

ومع ذلك وبغض النظر عن المقاربة التي نعتمد عليها، لا شك أن الإنترنت لا تشكل فقط وسيلة لتقريب الحكام من المحكومين في ظل مفهوم الديمقراطية الذي يعتمد على التمثيل و التفويض، ولكنها أيضا وسيلة لزيادة مشاركة المواطنين في الحياة السياسية للدولة[3].

---

[1] Marie-Christine Piatti, Les libertés individuelles à l'épreuve des NTIC, éd. Presse Universitaire de Lyon (PUL),
2001, p.28.

[2] Jonathan Bishop, « Increasing participation in online communities: A framework for human–computer interaction », Computers in Human Behavior, 23(2007), 1881–1893; Cliff Lampe, Erik Johnston, « Follow the (Slash) dot: Effects of Feedback on New Members in an Online Community, in International Conference on Supporting Group Work », GROUP '05, Sanibel Island, ACM Press.

[3] حول الروابط بين تكنولوجيا المعلومات والاتصالات والديمقراطية، أنظر:
Thierry Vedel, introductin au séminaire « La démocratie électronique. Visions, pratiques, significations » CEVIPOF, Paris, 1998 ; Pierre Chambat, « La démocratie assistée par l'ordinateur », Cahiers Politiques, n°4, Paris, L'Harmattan, p. 46–80.

ثانيا: الإنترنت كأداة للتحولات النظامية الحالية.

استنادا إلى ما تم مناقشته أعلاه وفي المجتمع المعاصر أين تخضع السياسة لتغطية إعلامية فورية، تلعب الإنترنت دورا خاصا في سياق التطورات الديمقراطية الحالية. من جهة وكما رأينا للتو فإنها تساهم في مشاركة مستخدمي الإنترنت في الحياة السياسية كمواطنين، ومن جهة أخرى فإنها توفر منبرا جديدا للنقابات ونشطاء جمعيات الدفاع عن حقوق الإنسان حيث يشكل أداة قيّمة في البلدان التي تكون فيها حرية التعبير معرضة للخطر[1].

حتى ان هناك حديث عن "معارضين إلكترونيين" وهم الأشخاص الذين يستخدمون الإنترنت كأداة للمقاومة و العمل من أجل معارضة أنظمة المراقبة[2].

في بعض الدول شهدنا هجمات في إطار حملة رقمية لمعارضة سياسات الحكومة. في روسيا تحاول السلطات بانتظام لزيادة المراقبة على الإنترنت بصورة قانونية، باسم مكافحة التطرف وحماية القصر، وكرد فعل اتخذ المعارضون لهذا النوع من المراقبة الرقمية، في إطار تجمعاتهم التقليدية، موجات

---

[1] « Freedom of speech is always the first casualty under a totalitarian regime. Such a regime cannot afford to allow the free circulation of information and ideas among its citizens. Censorship is the indispensable tool to regulate what the public may and what they may not know» écrit Lord Bridge, juge à la chambre des Lords, dans la decision Attorney General c/Guardian Newspaper Ltd. [1987] 1 WLR 1248. En effet, l'objectif de la propagande menée par J.P. Goebbels, ministre de l'Education de la Troisième Reich, était « que le peuple commence à penser de manière uniforme ».

بالفعل لقد خاطبت الدعاية النازية بقيادة غوبلز (وزير الدعاية الألماني ابان حكم هتلر) المشاعر وتلاعبت بالعواطف فلم تترك للشعب فرصة التفكير الهادئ فتبلدت عقوله حتى كف عن التفكير سوى تفكير واحد.

[2] تظل إسراء عبد الفتاح من ألمع الأسماء الشابة التى أثرت في مصر أخيراً، فهي صاحبة الدعوة لإضراب 6 ابريل عام 2008 علي شبكة الانترنت.

من الهجمات المنسقة من أجل إستحالة الوصول أو تعديل محتوى مواقع الأخبار الوطنية التي تقوم بالدعاية لصالح الحكومة. وقعت إحدى هذه المبادرات عند إجراء الانتخابات التشريعية في 4 ديسمبر 2011 وعرض مشروع قانون على البرلمان الروسي يتضمن جملة من الأمور، من بينها إنشاء سجل وطني موّحد يضم المجالات ومواقع الويب التي تتضمن معلومات محظورة النشر في روسيا ("قائمة سوداء" للخدمات التي تعتبر "خطيرة" من قبل الحكومة)[1].

في السياق نفسه و بعد كشفه عن بعض التفاصيل من حرب العراق، يدافع موقع ويكيليكس الذي يدخل في إطار ظاهرة "النضال الرقمي"، عن أيديولوجية و عن أهداف سياسية، على الرغم من أن الدوافع مختلفة لأن الهدف هو مناداة والتأثير على الرأي العام. الصعوبة التي تصحب هذا النوع من السلوك هو أنه مثير للجدل بشكل خاص، وحتى عندما ينطوي على ارتكاب جريمة يعاقب عليها القانون، فإنه يلقى في نفس الوقت دعم شريحة واسعة من المجتمع. وعموما فإن البعض يعتبر المعارضة الرقمية عملا من أعمال الحرب أو الإرهاب أو العصيان المدني، في حين أن البعض الآخر يعتبرها حرية للتعبير و ضرورية من أجل مقاومة الاستبداد.

---

[1] أغلقت النسخة الروسية من موسوعة ويكيبيديا على شبكة الإنترنت موقعها في 10 جويلية 2012، في احتجاج ليوم واحد على ما قالت إنها خطط للرئيس الروسي فلاديمير بوتين لابتكار نسخته الخاصة من "سور الحماية الصيني العظيم"، لاعتراض سبيل المعارضة على الإنترنت. وتمنح تغييرات أدخلت على قانون المعلومات المسؤولين الحكوميين في روسيا سلطة طلب إغلاق صفحات الإنترنت دون أمر من المحكمة، عن طريق وضعها في القائمة السوداء، والصين لديها بعض الأساليب الأكثر فعالية لمنع المعارضة على شبكة الإنترنت والسيطرة بإحكام على ما تمكن مشاهدته. وبموجب التغييرات المقترحة، فإنه إذا لم يحذف صاحب موقع المحتوى الذي يعتبر غير مناسب فيمكن منع الوصول إلى الموقع بأكمله في روسيا. وقالت موسوعة ويكيبيديا الروسية في بيان إن هذه التعديلات قد تصبح أساسا لفرض رقابة حقيقية على شبكة الإنترنت، وتشكل قائمة محظورة بمواقع وعناوين بروتوكول الإنترنت (IP).

لكن و كما هو الحال مع العديد من الاختراعات فإن المنتدى العام الذي تشكله الانترنت هو ظاهرة ذات حدين. و بما أنه مكان التقاء جميع الفئات الاجتماعية، و يتوقف على الكيفية التي سيتم استخدامه بها، يمكن له أن يكون مصدرا لتنمية النقاش السياسي المحايد أو أن يكون ضده، بفتح الطريق لهيمنة النزعات الشعبوية والديماغوجية على سبيل المثال. و بالإضافة إلى ذلك فإنه في حين أن هذه الأداة في متناول الجميع و تبدو مناسبة تماما للأنظمة الديمقراطية، ليس هو الحال في الأنظمة السياسية الأخرى، وخاصة الاستبدادية منها. في الواقع أي تدابير متخذة من قبل الحكومة يكون أثرها فرض الرقابة بأي طريقة كانت، على المسار الحر لمحتوى الاتصالات الإلكترونية، يصرف الانترنت عن غرضها كفضاء ديمقراطي عام وقد يؤدي إلى تحويلها إلى أداة تحكم وتلاعب بالمواطنين. وبشكل أقل وضوحا، يكون أثر تدابير التصفية وعرقلة المحتوى الرقمي المتخذة في الدول الديمقراطية و التي تبررها على سبيل المثال بسياساتها في مجال مكافحة الجريمة أو حماية الأحداث. و أكثر وضوحا و ربما بشكل صادم، يكون أيضا أثر تدابير الرقابة من قبل الأنظمة الاستبدادية لمنع النقاش السياسي المفتوح، و عرقلة التواصل وكذا تنظيم الحركات المناهضة للحكام.

بالتأكيد أنه بالنسبة للأنظمة السياسية، التي يصفها البعض بأنها "حكومات قرصنة"، وفي محاولتها للحد من حرية التعبير عن الآراء و فرض الرقابة على الاعلام، من خلال مراقبة صارمة وضارة لوسائل الإعلام المختلفة، ليست بظاهرة حديثة أو خاصة بالإنترنت[1]. ما تغير مع شبكة الإنترنت هو أنه بفضل طابعها غير المادي فإنه يصعب تحديدها وطبيعتها العابرة للأوطان وقدرتها على نقل البيانات بسرعة لا مثيل لها، حيث يصعب السيطرة عليها في الواقع وعلى الرغم من كل القيود المفروضة، فإنه من غير الممكن السيطرة عليها بشكل كامل.

---

[1] أنظر مقال س. خالد: "الاجرام الالكتروني والثورة التونسية "، ص4، في إطار اليوم الدراسي "الانترنت، الثورة والتحول الديمقراطي"، 13 أفريل 2012، ..http://droitdu.net

ولهذه الأسباب و بالنسبة للشعوب في الأنظمة الاستبدادية المحرومة من الحق في التعبير و تبادل الآراء، أصبحت الانترنت وسيلة للمقاومة لا غنى عنها تبعث على الأمل[1].

في تونس على سبيل المثال و في عهد الرئيس زين العابدين بن علي كانت وسائل الإعلام تخضع لرقابة واسعة النطاق. وأمام هذا الوضع كانت الإنترنت على الرغم من بعض تدابير التصفية المتخذة، ساحة مفتوحة نسبيا لتبادل المعلومات والآراء حول قضايا النظام الاجتماعي والسياسي. ومن المعروف على نطاق واسع أن وفاة محمد البوعزيزي والانتفاضة التي تلت لم يكن متوقعا أن يكون لها ذلك التأثير في العالم لو لم تقم الشبكات الاجتماعية مثل الفيسبوك وتويتر أو يوتيوب ببث صور عن المظاهرات وعن عنف الشرطة ضد المتظاهرين السلميين[2].

و هناك أمثلة عديدة: في ربيع 2009 خرج عشرو آلاف شخص إلى شوارع مولدافيا للاحتجاج على فوز الشيوعيين في الانتخابات البرلمانية. هذا الرقم ربما كان مغايرا إذا لم يكن بإمكان المتظاهرين الاتصال على الفور ودون عوائق عبر الشبكات الاجتماعية. في إيران بعد الانتخابات الرئاسية عام 2009 و القمع الذي

---

[1] قامت جماعة أنونيمس بهجوم إلكتروني على عدة مواقع إسرائيلية حكومية للانتقام من إسرائيل والتضامن مع غزة خلال العدوان الإسرائيلي على غزة العام الماضي، وشملت الهجمات المواقع الإلكترونية لوزارة المالية والسفارة الإسرائيلية في الولايات المتحدة الأمريكية.

[2] "وبحسب تقرير لمعهد التنبؤ الاقتصادي لعالم البحر الأبيض المتوسط، الصادر في شهر أغسطس (آب) الماضي، فإن أكثر من 20 مليون عربي يستخدمون شبكة التواصل الاجتماعي «فيس بوك»، وإن الإنترنت كان بمثابة أرضية للمقاومة في خدمة الثورات التي شهدتها بعض الدول العربية أو ما بات يعرف بــ«الربيع العربي». وإن «فيس بوك» مثلا كمحرك للثورات العربية لعب دورا لا يستهان به، حيث سمح بالانتشار الشامل للمعلومة غير المراقبة، مستمدة من مستخدمي الإنترنت أنفسهم." محمد عجم، «تويتر» و«فيس بوك».. زعيما ثورات «الربيع العربي»، جريدة الشرق الأوسط، 2011/12/26.

تلى ذلك، كان الإنترنت عاملا أساسيا وحافزا للمعارضة الديمقراطية لدرجة أن شيرين عبادي إقترح منح الإنترنت جائزة نوبل للسلام. على الموقع الذي تم إنشاؤه بهذه المناسبة في عام 2010، كان بإمكاننا قراءة الآتي: "(...) إن الإنترنت هو أكثر بكثير من مجرد شبكة لأجهزة كمبيوتر. هي في المقام الأول شبكة من الأفراد. رجال و نساء من جميع أنحاء العالم متصلون مع بعضهم البعض [...]. الحوار والمشاركة و الاتصال مع الآخرين، كانت دائما الترياق الأكثر فعالية ضد الكراهية و الصراع. (...) ".

وأخيرا تعتبر الشبكات الاجتماعية أيضا أنها كانت محرك الثورة المصرية في 2011، حيث توجت العديد من المظاهرات في ميدان التحرير وبعد 18 يوما فقط، باستقالة الرئيس حسني مبارك[1].

ويترتب على ما سبق أن الحركات الاجتماعية والسياسية على الإنترنت ظهرت كفاعل رائد في الاضطرابات الكبرى التي شهدتها البلدان سعيا إلى الديمقراطية[2]، ولكن أيضا من قبل منظمات تسعى لأهداف الأخرى مثل ظاهرة تنظيم الدولة الإسلامية. و سيتم تحليل طرق المكافحة والدعاية والتجنيد التي ظهرت من خلال تطوير وسائل الاتصال الإلكترونية، بما في ذلك لصالح المنظمات الإرهابية، في وقت لاحق.

إذا كان الرئيس الأمريكي باراك أوباما الفائز برئاسيات أمريكا في 04 نوفمبر 2008 هو أول رئيس في العالم يحقق فوزا حاسما بفضل الإنترنت فإن

---

[1] Sihem Najar, « Le cyberactivisme au Maghreb et dans le monde arabe », actes de la deuxième réunion du programme de recherche sur « La communication virtuelle par l'Internet et les transformations des liens sociaux et des identités en Méditerranée », Sidi Bou Saïd, les 24 et 25 juin 2011, Paris, 2013.

[2] خالد الطراولي، دور الإعلام في إنجاح الثورات ونقضها، موقع الجزيرة الاخبارية.

الرئيسين التونسي زين العابدين بن علي، و المصري حسني مبارك هما أول رئيسين في العالم يخلعان من طرف الشعب بفضل الإنترنت، و الشبكات الاجتماعية. و ليس مستبعدا أن الرئيس القادم في أي بلد في العالم، هو رئيس يحسن إستغلال الإنترنت[1].

الحق في فضاء خاص في بيئة رقمية عامة بإمتياز.

الديناميكيات الاجتماعية الجديدة التي تطورت مع نشر تقنيات المعلومات والاتصال، تقوم بإشراك من جهة، احتمالات تتبع أنشطة الناس على الانترنت و من جهة أخرى، العناصر المقدمة من طرف الأشخاص أنفسهم في حركة واسعة النطاق لظاهرة "عرض الذات". إن الزيادة الكبيرة في تدفق البيانات العابرة للأوطان وإنشاء قواعد بيانات حقيقية تصاحب التحول الحالي للهياكل الاقتصادية والاجتماعية تعتمد بصفة كبيرة على الثقة في الأدوات التنظيمية الجديدة التي تضعها الدول والمنظمات. إنّ التحدي يكمن إذن في حماية الحياة الخاصة للأفراد الذين يعهدون بمعلوماتهم من خلال المشاركة في مجتمع المعلومات، حيث يعرضون هويتهم للخطر وكذا سمعتهم وسرية اتصالاتهم الرقمية، مع الأخذ بعين الاعتبار في نفس الوقت أن الإنترنت، ويجب أن تبقى، بيئة افتراضية مفتوحة و في متناول الجميع (فرع أول).

أما المحور الثاني من حماية الحياة الخاصة والحفاظ على خصوصية الأشخاص، وخارج الظهور على المنتدى العام المتمثل في الإنترنت. يتعلق الأمر إذن بتوفير ضمانات السرية لأولئك الذين يستخدمون الإنترنت في إرسال رسائل في الاطار الخاص إلى متلق محدد (فرع ثاني).

---

[1] د. محمد لعقاب، المواطن الرقمي: كيف ساعدت تكنولوجيا المعلومات الثورات العربية، دار هومة، الجزائر، ط2، 2013.

الحق في حرمة الحياة الخاصة على الانترنت: نحو الاعتراف بالحق في حماية البيانات الشخصية بهدف بناء هوية رقمية.

في مجتمع المعلومات وفي الحاضر المضطرب بما أحدثته الرقمنة، فإن الآمال المرجوة من التكنولوجيا تنمو بنفس الوتيرة مع تنامي المخاوف. ويرافق النضج المرتبط بالقدرات الجديدة التي تقدمها لنا تكنولوجيا المعلومات والاتصالات زيادة الشكوك والوعي بالتحديات التي يجب مواجهتها، ولا سيما فيما يتعلق بالحفاظ على الحيّز الخاص للأشخاص، والتي أصبحت تمثل ركائز الاقتصاد الرقمي[1]. في هذا السياق، تظهر حماية البيانات الشخصية كشرط أساسي للحفاظ على الحياة الخاصة للأشخاص(أولا)، مما يؤثر بالضرورة على عملية بناء هويتهم وسمعتهم الرقمية(ثانيا) ثم نتطرق في الأخير إلى الحق في التستر كجزء من فكرة حماية الحياة الخاصة للتحكم في استخدام البيانات الشخصية (ثالثا).

أولا: ميلاد الحق في حماية البيانات الشخصية.

في بداية الأمر كان هذا الحق يدخل ضمن حقوق الشخصية القانونية وحرمة الحياة الخاصة، و قد تطور الحق في حماية البيانات الشخصية على مر السنين ليتم الاعتراف به في النهاية كحق مستقل (1). لم يكتمل هذا التطور وذلك لأن الحق في حرمة الحياة الخاصة وفي حماية البيانات الشخصية، تواجه باستمرار

---

[1] في هذا الاتجاه: - Le Baromètre de l’INRIA 2014, « Les Français et le numérique. Bienvenue dans l’ère de l’homo numéricus ! Le pouvoir d’agir… en toute coscience », 2ème éd. mars 2014, adresse: https://www.inria.fr/content/.../Barometre2014_DOSSIER_PRESSE.pdf.

التحديات التي تفرضها الممارسات الجديدة المتعلقة بنقل البيانات دوليا والتي تشكل المبدأ الأساس في آلية عمل السوق الرقمي(2).

1- من الحق في الشخصية القانونية و في حرمة الحياة الخاصة إلى الاعتراف بحق مستقل.

الحق في الشخصية القانونية هو الأساس الأول لكل حماية تنسب اليوم للحيّز الخاص بالأفراد(أ). الاعتراف دوليا بالحق في حماية البيانات الشخصية تظهر في هذا السياق كجانب حديث من هذا الحق الذي يهدف إلى حماية خصوصية الحياة الشخصية، هذه الخصوصية التي تغيّرت حدودها بفعل تمدّد التقنيات الرقمية التي تفترض التطفل (ب).

أ- الحقوق اللصيقة بالشخصية كمصدر للحق في حماية الحياة الخاصة.

حماية وجود الفرد في الشبكة الرقمية تشكل "اقليم جديد للحقوق اللصيقة بالشخصية"[1]. يمكن تعريف الشخصية بـــ"الفرد أي جميع جوانب الشخص التي تميزه عن كل أشباهه في الماضي أو الحاضر أو المستقبل."[2] و إن الحقوق التي تتعلق بهذا المفهوم تعني "كل الحقوق التي يعترف بها القانون لأي شخص، من حيث أنها صفات لا تنفصل عن شخصيته مثل الحق في الحياة و في السلامة الجسدية، و الحق في الشرف و الصورة، والحق في احترام قرينة البراءة. و هي حقوق غير مالية، و ذات حجية مطلقة"[3].

---

[1] Laure Maude, « Les nouveaux territoires des droits de la personnalité », Gaz. Pal., 18-19 mai 2007, p. 22.

[2] Bernard Beignier, « Le droit de la personnalité », PUF, Que sais-je ?, 1992.

[3] Lexique des termes juridiques, 19ème éd., Dalloz 2012, p. 305.

كما عرّفها أيضا جيرار كورنو على أنها "الحقوق المتأصلة في شخصية الإنسان و التي يتمتع بها كل شخص طبيعي (فطرية وغير قابلة للتصرف) لحماية مصالحه الأساسية"[1]. ولذلك فإن أي محاولة لحماية ما تمثله الشخصية يجب أن ترتبط بحماية تنوع الطبيعة البشرية من الطابع التمييزي للعناصر المكونة للفرد في حد ذاته. سيتعلق الأمر إذا بحماية حريته في الوجود و كرامته. وعلاوة على ذلك فرغم اقترابها من مصطلح الحرية فإنه لا يجب أن تماثله، لأن الحقوق اللصيقة بالشخصية "في حدود الحق الشخصي" قريبة من الحريات حيث يتمتع بها جميع البشر، لكنها تختلف عنها في أنها تنشئ منطقة محمية "تستثني منافسة الغير"[2].

في فرنسا كان الأستاذ ريمون ساليّ أول من تطرق إلى مفهوم الحقوق اللصيقة بالشخصية في " دراسة نظرية الالتزام في مشروع القانون المدني الألماني" التي نشرت سنة 1890[3]. و بالنسبة إليه فإن الحقوق اللصيقة بالشخصية هي في مفترق طرق بين القانون المدني و القانون الجنائي و حقوق الإنسان. و يمثل الحفاظ عليها موازنة قضائية بين حماية الشخص و قيم أخرى مثل حرية التعبير أو ضرورة الإثبات[4].

---

[1] Gérard Cornu, « Vocabulaire juridique », 8ème éd., p 679.

[2] Gilles Goubeaux, « Les personnes, Traité de droit civil, Les personnes », LGDJ, n° 280 et s.

[3] Raymond Saleilles, « Essai d’une théorie de l’obligation d’après le projet de code civil allemand », Hachette Livre BNF, 2012 ; v. ég. Bernard Beignier, « L’honneur et le droit », LGDJ 1995, p. 45 ; D. Talion, « Les droits de la personnalité », Responsabilité civile, n° 2.

[4] Jean-Christophe Saint-Paul, « Droit de la personnalité », LexisNexis, 2013. Egal. Marc Domingo, « Protection de la vie privée et liberté des médias », Gaz. Pal., 30-31 déc. 1994 ; Emmanuel Pierrat, « Protection des droits de la personnalité », Legicom, n° 2, 1996, p. 87-93.

إن الحق في حرمة الحياة الخاصة للفرد عنصر أساسي في الحقوق اللصيقة بالشخصية، متى كان موضوع هذا الحق هو الشخصية الانسانية الفريدة.

في هذا السياق اعترف الاجتهاد القضائي في أوروبا وفي وقت مبكر جدا بـــ "حق أعم في حرمة الحياة الخاصة"[1] من خلال قرارات بشأن سرية المراسلات[2] و الحق في الصورة[3].

فيما بعد إعترفت محكمة العدل الأوروبية في عام 1969 بالحق في الحياة الخاصة كمبدأ عام من مبادئ القانون الأوروبي، و ذلك بضمان إحترامه[4]. في وقت لاحق اعتبر القاضي الفرنسي أن الحق في حماية الحياة الخاصة هو "حق الشخص في أن يكون حرا في أن يعيش حياته كما يشاء مع الحد الأدنى من التدخل الخارجي"[5].

---

[1] Pierre Kayser, « Les droits de la personnalité: Aspects théoriques et pratiques », p. 78, n° 69.

[2] Raymond Lindon, « Les droits de la personnalité. Dictionnaire juridique », 1993, verbo Lettres confidentielles, p. 135.

[3] في هذا الاتجاه:

Trib. de la Seine, 16 juin 1858, Raymond. Lindon, « Dictionnaire juridique », Les droits de la personnalité, 1983, Dalloz, p. 248 et 249 ; Cass. Civ. Rej. 14 mars 1900, D. 1900.I.497, note Planiol: à propos du refus du peintre de livrer un portrait au commanditaire, l'artiste ne peut en faire « un usage quelconque avant d'en avoir modifié l'aspect, de manière à le rendre méconnaissable ». Ainsi, même si la reproduction de l'image d'une personne est réalisée avec son consentement, celle-ci conserve des droits sur cette reproduction et l'usage qui en est fait.

[4] CJCE, n° 29-69, Stauder c/ Ville d'Ulm, 12 nov. 1969.

[5] CA Paris, 15 mai 1970, épx Tenebaum, alias J. Ferrat: D. 1970, p. 466, concl. Cabannes, note P. A. et H. M.

بعيدا عن هذا الاجتهاد القضائي المتذبذب وغير المستقر، فإن التشريعات المعتمدة في هذا المجال هي الأخرى لا تقدّم حلولا موحدة. في أوروبا تظهر اختلافات هامة على سبيل المثال بين اسبانيا التي أدرجت مفهوم الحياة الخاصة في دستورها لسنة 1978[1] و « *right of privacy* » "الحق في الخصوصية" الأنجلوسكسوني. فقبل اعتماد قانون حقوق الانسان « *Human Right Act* » سنة 1998، وبعد الاطلاع على القرارات الصادرة عن محكمة الاستئناف في لندن، ندرك أنه بالنسبة للقضاة "لا يوجد أي حماية للحياة الخاصة"[2] في القانون البريطاني.

في الولايات المتحدة الأمريكية يعتبر البند الأول أساس الحريات الفردية، وعلى خلاف ذلك جاء الاعتراف الدستوري بالحياة الخاصة أكثر تشتتا. ونظرا لغموض مفهوم الحياة الخاصة لم يتم النص عليه في الدستور الأمريكي. و في غياب أساس تشريعي استخدم القاضي الأمريكي في البداية البند الرابع والخامس لضمان حظر التفتيش والحجز التعسفي والحفاظ على الضمانات الإجرائية الممنوحة للأفراد. يعتبر بندان من الدستور الأميركي حاليا كأسس رئيسية لحماية

---

[1] المادة 18 من الدستور الإسباني لسنة 1978 : يتم ضمان حق الشرف وحق الحرمة الشخصية والعائلية وحق الحفاظ على السمعة.
لا تنتهك حرمة المسكن. ولا يجوز دخوله أو تفتيشه إلا بإذن صاحبه أو بموجب قرار قضائي إلا في حالة التلبس بالجريمة.
تم ضمان سرية الاتصالات وخصوصاً البريدية والتلغرافية والهاتفية ما عدا في حالة صدور قرار قضائي.
يقيد القانون مجال استعمال المعلومات لضمان حق الشرف وحق الحرمة الشخصية والعائلية للمواطنين ولضمان الممارسة التامة لحقوقهم.

[2] Cour d'appel de Londres, affaire Kaye c/ Robertson, 23 févr. 1990: « it is well known that in English law there is no right to privacy ».

الحياة الخاصة، بفضل تفسيرات جريئة قدّمها القضاة. ويتعلق الأمر بالبند التاسع والرابع عشر، و ينص البند التاسع " إن القرارات التطبيقية لهذا الدستور المتعلقة بالحقوق الثابتة والأساسية لا يجب إجراء تعديل فيها قد يغير أو يحطم الحقوق الأخرى المحفوظة للشعب. "، و يتضمن البند الرابع عشر التزام الأمن القانوني (due process clause).

بشكل عام ونظرا لعدم وجود تعريف قانوني يمكن اقتراح تعريف مجرد للحياة الخاصة، والتي يمكن تلخيصها في تعريفات كل من الفقه الأمريكى والفرنسي والمصري والتي جاءت في شكل وصفي، و ذلك على النحو الآتي:

يعرّف فريق من الفقه الأمريكى الحق فى الحياة الخاصة بأنه أحيانا: "الحق فى الخلوة"، حيث أنه من حق الشخص المطلق أن يلزم الغير أن يتركه و شأنه[1] و لا يعكر عليه هذا الغير صفو خلوته[2]. أكثر من ذلك فإنا البعض من الفقه يصل إلى اعتباره حق الشخص في أن لا يكون اجتماعيا[3].

في فرنسا نذكر أهم و أبرز الفقهاء ممن حاولوا إعطاء تعريف للحياة الخاصة بشكل واسع، حيث عرّفها كربونيه على أنها "حق الشخص في أن يترك في هدوء وسكينة"[4] و الفقيه نفسه أضاف فى موضع آخر بأنها: "المجال السرّي الذي يملك

---

[1] قد ذهب القاضيان الأمريكيان **Warren** و Brandeis في عام **1890** إلى أن تعريف الخصوصية بأنها : (**الحق** في أن يترك الشخص وحيدا)، ولهذا فإن الخصوصية وفق هذا الفهم تعدو أهم سمة من سمات الحرية في المجتمع الديمقراطي.

« The right to privacy », Harvard law review, 1890 p 193 année.

[2] Louis NIZER: "The right of privacy: a half century's developments", Michigan law, Rev. 1941 Vol. 39, p 526.

[3] Leon BRITTAN: "The right of privacy in England and the United States of America", Tulane Law review, 1981, p 203.

[4] Jean CARBONNIER, op.cit, N° 86 bis, p 254 où définit la vie privée comme étant "Le droit de l'individu à être laissé dans la tranquillité et la paix".

للفرد بشأنه سلطة استبعاد أي تدخل من الغير وهي حق الشخص في أن يترك هادئا"[1].

فى مصر مال جانب من الفقه إلى تحديد الحق فى الحياة الخاصة وفقا لمفهوم الحرّية، من ذلك تعريف أحدهم لها بأنّها " حق الفرد فى أن يحدّد لنفسه مدى مشاركة الآخرين له فى أفكاره و سلوكه إلى جانب الوقائع المتعلّقة بحياته الشخصية، وهو حق طبيعى و أساسى فى مواجهة الدولة والأفراد لضمان كرامة الفرد و حريّته فى تحديد مصيره"[2].

في ظل الغياب الشبه الكامل لآراء فقهية في الجزائر حول موضوع الحق في الحياة الخاصة، يرى البعض ضرورة وضع إطار لهذا الحق يترك فيه للفرد الحريّة اللازمة وليست الكافية، أين يظهر من خلالها إرادته فى اختيار نمط عيش خاص خارج النمط الاجتماعى يراه مناسبا له، يمكّنه من الانزواء تحقيقا لقسط من الرّاحة النفسية سواء شاركه فيه جمع من الأفراد قبلهم هو أم استبعد الكلّ. هذا النمط الذي يتبناه الفرد بصفة مؤقتة أم بصفة دائمة يمنع على الكافة – أفراد كانوا أم سلطات – التدخل فيه و اختراقه دون إذن منه طالما بقى هو فى إطاره محترما للشّرع و القانون.

فكما أنّ للفرد ضرورة ماسة وحيوية لأن يختلط بالجماعة من أجل توازن و انسجام و راحة نفسيّة، بالمقابل وللغرض نفسه نظهر الضرورة الحيوية لأن ينعزل مؤقّتا و يبتعد عن الضغوط و الالتزامات الاجتماعية. من هذا المنظور و

---

[1] Jean CARBONNIER, op.cit, p 124.

[2] د/ محمد عبد العظيم محمد، حرمة الحياة الخاصة في ظل التطور العلمي الحديث، رسالة دكتوراه، جامعة القاهرة، كليّة الحقوق، 1988، ص 413.

فقط من هذا المنظور يكون حقه المطلق فى حرمة حياة خاصة تقتضي حماية شرعية و قانونية كاملة و واجبة[1].

و في ضوء ما سبق تمّ تكريس الحق في الحياة الخاصة أولا بموجب المادة 12 من الإعلان العالمي لحقوق الانسان، ثم بموجب المادة 8 من الإتفاقية الأوروبية لحقوق الانسان، التي تضمن لكل فرد الحق في احترام حياته الخاصة و الأسرية، ومنزله ومراسلاته. كما تحمي هذه المادة الفرد من التدخلات التعسفية من قبل السلطات العامة – من طرفهم فقط – في حياته الخاصة. و بالتالي لا يتم تقبلها إلا كتدابير استثنائية منصوص عليها صراحة في القانون و ضرورية في مجتمع ديمقراطي حماية للنظام العام و حقوق الفرد. وحده إذن تدخل السلطة العامة يكون بموجب نص.

تم تبني نفس التصور في فرنسا حيث نصت المادة 9 من القانون المدني التي أدرجها قانون 17 جويلية 1970 على حق كل شخص "في احترام حياته الخاصة"[2]. كما أقرّ المجلس الدستوري الفرنسي بعد ذلك صراحة بأن الحرية الفردية هي مصدر الحق في حماية الحياة الخاصة[3]، بحيث أن أي مساس بهذا الحق من المرجح أن يؤدي إلى المساس بالحرية الفردية[1].

---

[1] د/ صفية بشاتن، الحماية القانونية للحياة الخاصة دراسة مقارنة، رسالة دكتوراه، جامعة تيزي وزو، كليّة الحقوق، 2012، ص 89.

[2] Pour Jean Carbonnier, une telle formulation du droit à la vie privée s'apparente au droit à la tranquillité. V. Jean Carbonnier, « Droit civil », vol. 1, PUF, 2004, p. 518. V. Emmanuel Dreyer, « Le respect de la vie privée, objet d'un droit fondamental », Comm. Comm. Électr. 2005, ét. n° 18, spéc. § 15 ; Laure Marino, « Les nouveaux territoires des droits de la personnalité », Gaz. Pal. n° 139, mai 2007, p. 22.

[3] Cons. Const. N° 99-416 DC, 23 juill. 1999. Dans le considérant 45 sur la carte vitale lu juge estime que « la liberté proclamée par l'art. 2 de la Déclaration des droits de l'homme et du citoyen implique le respect de la

من هنا يمكن تحديد التزام مزدوج يقع على عاتق الحكومات: يتمثل من جهة في عدم التدخل التعسفي في خصوصية مواطنيها، و من جهة ثانية إتخاذ جميع التدابير اللازمة لردع انتهاك حرمة الحياة الخاصة لمواطنيها من طرف الغير[2]. و تم تكريس هذا الالتزام الإيجابي في وقت لاحق في مجال البيانات الشخصية من طرف محكمة حقوق الإنسان الأوروبية (CEDH)، والتي لم تكتفي بالتأكيد فقط على إلتزام عدم التدخل غير الشرعي في بيانات الأفراد، و لكن ذهبت إلى أبعد من ذلك باستنباط التزامات حقيقية تتحملها الدول[3].

و نتيجة لذلك قامت بعض الدول بتكييف تشريعاتها لضمان احترام التزاماتها على نحو أفضل في مجال حماية البيانات الشخصية. في فرنسا تم سن قانون "المعلوماتية والحريات"، و الذي سوف نتعرض إليه لاحقا، حيث أسّس لحماية الحياة الخاصة حصريا في إطار العلاقة بين المواطن و الادارة. لكن حاليا "التمييز بين القطاعين العام والخاص لم يعد مناسبا، حيث يسعى القطاع الخاص

---

vie privée ». V. D. 2000, p. 265, obs. Marino ; Comm., comm. électr. 1999, comm. 52, note Desgorges ; RTD civ. 1999, p. 725, obs. N. Molfessis.

[1] Cons. const., 18 janv. 1995, n° 94-352 DC: JO du 21 janv. 1995 ; Cons. const., 23 juill. 1999, n° 99-416 DC: JO du 28 juill.1999; Cons. const., 9 nov. 1999, n° 99-419 DC: JO du 16 nov.1999.

[2]: في هذا الاتجاه

CEDH, Marckx c/ Belgique, n° 6833/74, 13 juin 1979, relatif à la filiation et aux droits des successions, série A, n° 31, JT, 1979, 513, obs. F. Rigaux ; AFDI, 1980, 317, obs. Pelloux ; JDI, 1982, 183, obs.

[3] CEDH Gaskin c/ Royaume-Uni, 7 juill. 1989, req. N° 10454/83, série A, n° 160.

أيضا إلى معرفة كل شيء عن مستخدمي الانترنت. لم يعد لقب "الأخ الأكبر *Big Brother*" منحصرا فقط في الدولة[1].

في نهاية المطاف فإن حرمة الحياة الخاصة حق نسبي. فمن اللحظة التي يقوم فيها الشخص برسم حدود ما يدخل في إطار حياته الخاصة، وجب أن تكون هذه الأخيرة محمية بعد أن اعتبرها لصيقة بشخصيته[2]. وذلك وفقا لازدواجية مكرسة قانونا، والتي تحكم إما العلاقة بين المواطن والحكومة أو بين الأفراد أنفسهم – ولهذه الأخيرة أهمية خاصة أمام تحدي إمكانية انتهاك حرمة الحياة الخاصة للأفراد من طرف مزودي خدمات الإنترنت.

ب- استقلال الحق في حماية البيانات الشخصية على المستوى الدولي.

الاعتراف بالجانب "الخصوصي" للحق في احترام الحياة الخاصة يرافقه تطوّر البعد المعلوماتي لهذا الحق. في الواقع وبنشر المعلومات حول الأشخاص في النصف الثاني من القرن العشرين، بدأ الكشف عن المخاطر التي يشكلها الغير على الفرد – مثل صاحب العمل، مدير البنك، شركة التأمين، الخ وبالتالي لم تعد السلطة العامة المصدر الوحيد للمساس بالحياة الخاصة، ولكن أيضا الخواص أكثر فأكثر حيث من المحتمل أن يستخدموا المعلومات المتعلقة بالجوانب الخاصة بحياة الأفراد تعرض للخطر حرياتهم وقدرتهم في الحفاظ على سرية بعض الأشياء[3].

في أوروبا تم في بداية الأمر ربط حماية البيانات بالحرية الشخصية. على سبيل المثال ومن خلال المادة 2 و4 من الاعلان العالمي لحقوق الانسان

---

[1] C. Chassigneux, « Vie privée et commerce électronique », Thémis, Montréal, 2004, p. 128-129.

[2] Laure Marino, « Les nouveaux territoires des droits de la personnalité », précité.

[3] M. Contamine-Raynaud, « Le secret de la vie privée, ouvrage collectif, L'information en droit privé », LGDJ, 1978, p. 454, n° 36.

والمواطن، سعى القاضي الدستوري الفرنسي إلى حماية حرية الأفراد من خلال حماية البيانات الشخصية من الاستخدام التعسفي[1]. وفي وقت لاحق تم ربط هذه الحماية بفكرة الحياة الخاصة، والمستمدة أيضا من الحرية الفردية.

بشكل عام فإن النتيجة اللازمة لقبول معالجة البيانات هي بطبيعة الحال حماية هذه البيانات. من حيث المبدأ وحتى يتم معالجتها بشكل قانوني، يجب جمع البيانات على أساس مجموعة من المبادئ التي تكفل حماية الأشخاص. هذا هو إذن الهدف الأولي للقوانين المتعلقة بمجال البيانات الشخصية.

يُعرّف دوليا بأنه " حق الأفراد في معرفة كيفية معالجة البيانات التي تحدد هويتهم، وكذلك الضمانات المرتبطة بهذه المعالجة "[2]، أصبحت هذه الحماية موضوعا لتشريع خاص. يعود ادراكها بشكل مستقل و للمرة الأولى في قانون ألماني في اقليم هيس Land of Hesse[3] وتبعه في السويد القانون الوطني الأول في حماية البيانات بعد ذلك في عام 1973[4]. بعد مرور 40 عاما، وفي عام 2012 تم تعداد حوالي 89 قانون وطني في هذا المجال[5]. و تختلف الأساليب التنظيمية و ذلك حسب السياقات القانونية و الإدارية و الثقافية لكل بلد، و كذا المبادئ المطبقة والتي تشكلت تدريجيا وفقا للتراث التاريخي والفلسفي

---

[1] Cons. Const., 25 juill. 1991, Accords de Schengen, n° 91-294 DC, Rec., p.91, RJC, p. I-455.

[2] Christopher Kuner, « An international legal framework for data protection: issues and prospects », 2009, 25 CLSR, 307, 308.

[3] قانون ألماني في اقليم هيس Land of Hesse الصادر في 07 أكتوبر 1970.

[4] القانون السويدي لحماية البيانات الشخصية الصادر في 11 ماي 1973.

[5] Graham Greenleaf, « Global Data Privacy Laws: 89 Countries, and Accelerating », Privacy Laws & Business International Report, n°115, févr. 2012, Queen Mary School of Law Legal Studies Research Paper, n° 98/2012.

والاجتماعي والثقافي الذي يميّز كل بلد. ذلك في حين أن بعض الدول قد وضعت آليات إدارية، والبعض الآخر أعلن عن مدونات حسن سلوك بهدف منع انتهاك الحقوق الأساسية للأشخاص[1].

يمكن استنباط مجموعة من الضمانات كقاسم مشترك لجميع النصوص المعتمدة، على الأقل في التقاليد الأوروبية. و من بين هذه الضمانات نجد بصفة خاصة استيفاء شرط موافقة الشخص الذي تعالج بياناته. ضمانات أخرى متعلقة بجودة البيانات، أي قد تم الحصول عليها بطريق مشروع و قانوني و تستخدم للغرض الأصلي المعلن والمحدد[2] و لا تكشف لغير المصرح لهم بالاطلاع عليها تتصل بالغرض المقصود من الجمع و لا تتجاوزه و محصورة بذلك و تتلف عند استنفاذ الغرض من جمعها.

ومن المتفق عليه أنه باستثناء الحالات المنصوص عليها قانونا، ينبغي أن يتم حظر جمع البيانات "الحسّاسة". و وفقا للنصوص نجد مجموعة من الحقوق التي يتمتع بها الأشخاص على بياناتهم و تتمثل في الحق في الوصول إليها مع حق الإخطار بأنشطة المعالجة أو النقل و حق التصحيح والتعديل وحتى طلب الالغاء. العنصر الأخير في اطار هذا القاسم المشترك يتمثل في التزام الجهة المسؤولة عن المعالجة بمعايير أمن ملائمة لحماية المعلومات و نظم المعالجة. و في الأخير

---

[1] ففي السويد وألمانيا على سبيل المثال، كانت الطريقة المتبعة هي إنشاء لجان ومكاتب إدارية مخول لها بتسجيل قواعد البيانات، ومراقبة تشغيل هذه الأنظمة من خلال إجراءات ترخيص وإنشاء أنواع مختلفة من الوسطاء أو آليات للطعن على الصعيد الوطني، أو على مستوى المقاطعات في الحالة الألمانية. ومن ناحية أخرى أخذت حماية البيانات في بريطانيا العظمى شكل مدونة لقواعد الممارسة الجيدة للمنظمات المشاركة فى الاقتصاد الرقمى.

[2] الغرض "المحدد و المشروع" المنصوص عليه فى الاتفاقية الأوروبية رقم 108 المتعلقة بحماية الأشخاص الذاتيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي الموقعة بستراسبورغ في 28 جانفي 1981.

فإن الهيئات المستقلة المكلفة بمراقبة مدى احترام الضمانات المذكورة أعلاه، يتم إنشائها من طرف الدول.

وعلى الصعيد الدولي فإن الاهتمام بحماية البيانات الشخصية من طرف الأمم المتحدة جاء متأخرا، في أعقاب اعتماد النصوص العامة من طرف منظمة التعاون والتنمية الاقتصادية OCDE[1] و مجلس أوروبا[2].

و في هذا الاتجاه نص الدستور الجزائري المعدّل بموجب القانون رقم 01/16 المؤرخ في 06 مارس 2016[3] على حماية البيانات الشخصية في المادة 46 حيث نصت على أنه " لا يجوز انتهاك حُرمة حياة المواطن الخاصة، وحرمة شرفـــه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم. حماية الأفراد في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه ". تجدر الاشارة إلى أنه سوف يتم مناقشة مشروع القانون المذكور في هذه المادة بشأن حماية البيانات الشخصية في الأيام المقبلة من طرف الحكومة[4] والذي سيتضمن بالتأكيد ما بلورته التجربة الأوروبية في هذا المجال.

---

[1] المبادئ التوجيهية لحماية الخصوصية والتدفقات عبر الحدود للبيانات الشخصية التي تم تبنيها في 23 سبتمبر 1980، وهي مستوحاة من Code of Fair Information Practices الأمريكي لعام 1973.

[2] اتفاقية المجلس الأوروبي لحماية الأفراد في مواجهة المعالجة الآلية للبيانات الشخصية STCE n° 108 الموقعة في 28 جانفي 1981، ستراسبورغ. ودخلت الاتفاقية حيز التنفيذ في 1 أكتوبر 1985 بعد 5 تصديقات. وتتعلق حاليا بأكثر من 40 جهة. وقد عزز بروتوكول n° STE 181 المؤرخ في 8 نوفمبر 2001 الموقع في ستراسبورغ التزامات الأطراف الموقعة بإلزامها على إنشاء سلطات رقابة وضمان دورها.

[3] القانون رقم 16-01 مؤرخ في 26 جمادى الاولى عام 1437 الموافق ل 6 مارس. سنة 2016 يتضمن التعديل الدستوري.

[4] وكالة الأنباء الجزائرية، الحكومة ستناقش "قريبا" مشروع قانون متعلق بحماية المعطيات الشخصية، 15 أكتوبر 2017.

لكن كما سنرى أدناه فإن الاشكالية الرئيسية لحماية البيانات الشخصية في الوقت الراهن تتمثل في عدم وجود توافق بين النظام المعمول به في أوروبا و في الولايات المتحدة الأمريكية، و هما الفاعلان الرئيسيان في الاقتصاد الرقمي الذي يشكل فيه هذا النوع من البيانات قيمة أساسية.

2- حماية الحياة الخاصة والبيانات الشخصية أمام تحدي نقل البيانات في إطار الاقتصاد الرقمي.

أدى التسويق الالكتروني للسلع و الخدمات الذي يصاحب الثورة الرقمية إلى زيادة تدفق البيانات دوليا. بالفعل فمنذ اللحظة التي قامت فيها الابتكارات التكنولوجية مثل الحوسبة السحابية Cloud computing أو البيانات الضخمة Big Data بتحويل معالجات البيانات التقليدية نحو "جهات معالجة متنوعة مكلّفة بمهام متعددة و لها مسؤوليات معقدة"[1]، جعلت معالجة و تخزين و نقل البيانات أسهل و أسرع و أرخص مما كانت عليه في الماضي[2]. حيث أصبح تدفق البيانات بين مختلف الدول يتم على نطاق شامل اليوم من حيث أن تقاسم الأدوات وتبادل المعلومات يستند بالضرورة إلى نقل بيانات[3].

في هذا السياق فإنه يجب على القواعد المعتمدة في مجال حماية البيانات مواجهة التحديات المتعلقة بالتحولات التي طرأت على النماذج الاقتصادية و على

---

[1] De Hert Paul and Vagelis Papakonstantinou. “The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals.” Computer Law & Security Review, Volume 28, p. 130-131.

[2] Michael Birnhack, « The EU Data Protection Directive: An engine of a global regime », 2008, 24 CLSR, p. 508-510.

[3] Éric A. Caprioli, « Les flux transfrontières des données à caractère personnel en matière bancaire », RDBI., 2010, n°1, p 72.

أنماط الإنتاج و في استخدام البيانات. بالفعل فالحوسبة السحابية Cloud computing لا تتمثل في القيام بمعالجات في الخوادم الداخلية internes serveurs للشركة، و لكن في خوادم خارجية تدار من طرف مقدمي الخدمات مثل جوجل و أمازون أو ميكروسوفت.

هذه الخوادم الضخمة Méga–serveurs موزّعة في جميع أنحاء العالم، دون معرفة في أي منها بالضبط و في أي لحظة توجد البيانات. يصبح إذن الالتزام بمنع تصدير البيانات الشخصية معقدا بشكل خاص، إلا إذا إستطاع مقدم الخدمة تحديد مكان خوادمه بدقة[1]. لذا فإن فعالية القواعد التي تحكم نقل البيانات على المحك أمام الطبيعة غير الملموسة و العابرة للحدود لكل من الجهات الفاعلة و العالم الافتراضي الذي تنشط فيه.

ونتيجة لذلك فإن الاشكالية الرئيسية في النصوص الدولية الحالية التي يكون الغرض منها حماية البيانات الشخصية تتمثل في تأطير نقل البيانات عبر الحدود، و لكن دون أن يمنع ذلك التدفق الحر للبيانات و الذي يعتبر أساس تطور الاقتصاد الرقمي.

وبشكل أكثر تحديدا فإن "نقل البيانات" يجب أن يفهم على أنه " إرسال، توصيل أو تبادل البيانات التي تكون أو المعدّة إلى أن تكون محل معالجة، بغض النظر عن الوسيلة المستخدمة – وإن كانت معظمها إلكترونية – من داخل دولة عضو في الاتحاد الأوروبي إلى بلد آخر – ليس بعضو في الاتحاد الأوروبي أو المنطقة الاقتصادية الأوروبية "[2].

---

[1] Fabrice Mattatia, « Traitement des données personnelles. Le guide juridique », Eyrolles, 2013, p. 19.

[2] Christine CAUSSE GABARROU, « Les transferts de données à caractère personnel dans la proposition de Règlement du Parlement

بين مختلف القوانين الوطنية المتعلقة بحماية البيانات، عرفت مسألة نقل البيانات الشخصية في الشبكات الرقمية قفزة نوعية في أعقاب هجمات 11 سبتمبر 2001 الإرهابية في الولايات المتحدة الأمريكية، وكانت النتيجة زيادة في ممارسات المراقبة العامة لأنظمة الاتصالات لضمان الأمن الدولي. وجاءت هذه االقفزة كرد فعل لحقيقة أن السلطات الحكومية في محاربتها للاجرام الإلكتروني المتزايد، أهملت بطريقة أو بأخرى ضرورة حماية الحياة الخاصة للمواطنين، و يتجلى ذلك من خلال الغياب المطلق لكل ما له صلة بحماية البيانات الشخصية في اتفاقية المجلس الأوروبي المتعلقة بمكافحة الجريمة الالكترونية الموقعة في بودابست في 23 نوفمبر 2001[1].

وبالتالي "عندما يوفر التشريع في بلدين أو عدة بلدان معنية بتدفق البيانات عبر الحدود ضمانات متساوية فيما يتعلق بحماية الحياة الخاصة، ينبغي أن يكون بالإمكان أن تنتقل المعلومات بنفس الحرية التي تنتقل بها في كل اقليم من الأقاليم المعنية. في حالة عدم وجود ضمانات مماثلة، لا يجوز فرض قيود على هذا

---

européen et du Conseil et compétitivité des entreprises: perspectives d'amélioration », RLDI, 2013, n° 98.

[1] فيما يتعلق بهذه الاتفاقية أنظر:

Abraham D. Sofaer, « Toward an International Convention on Cyber » in Abraham D. Sofaer, Seymour Goodman, « The Transnational Dimension of Cyber Crime and Terror », p. 225, adresse: http://media.hoover.org/documents/0817999825_221.pdf ; Marco Gercke, « The Slow Awake of a Global Approach Against Cybercrime », CLRI, 2006, p. 140 et s.; Marco Gercke, « National, Regional and International Approaches in the Fight Against Cybercrime », CLRI, 2008, p. 7 et s.; Richard Jones, « The Council of Europe Convention on Cybercrime, Themes and Critiques », 2005, adresse: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf.

الانتقال على نحو غير شرعي و فقط بقدر ما تقتضيه حماية الحياة الخاصة "[1].
تؤكد الأمم المتحدة بذلك على المبدأ الذي سبق تكريسه بموجب الاتفاقية رقم 108 و المتمثل في "الحماية المتكافئة"، تم النص عليه أيضا في التوجيه الأوروبي لسنة 1995 تحت تسمية " الحماية الملائمة ". وفقا لهذا المبدأ الأوروبي للحماية الملائمة فإن التدفق الحر للبيانات مضمون فقط فيما يتعلق بنقل البيانات بين الدول التي تتوفر على قواعد قانونية تضمن مستوى كاف من الحماية[2].

وبالنسبة للحالات الأخرى وفي حالة عدم وجود ضمانات كافية فإن نقل البيانات محظور (في فرنسا تنص على هذا المنع المادة 68 من قانون المعلوماتية و الحريات).

ومع ذلك فقد تم تبني مقاربة معاكسة من خلال المبادئ التوجيهية لمنظمة التعاون و التنمية الاقتصادية و كذا بعض التشريعات الوطنية – مثل نيوزيلندا أو أول قانون لحماية البيانات Data Protection Act في بريطانيا لسنة 1984. و وفقا لهذه النصوص فإن عمليات النقل الدولي للبيانات مسموح به ضمنيا، إلا في الحالات التي تشكل خطرا معينا، مثل نقل "البيانات الحساسة، و التسويق المباشر أو القرارات الفردية المعالجة آليا "[3]

---

[1] قرار الجمعية العامة للأمم المتحدة 95/45 المذكور سابقا.

[2] وفي هذا السياق يعتبر مستوى الحماية كافيا في جميع الدول الأعضاء في الاتحاد الأوروبي. ومن ناحية أخرى من المهم التمييز بين هذين المفهومين للحماية المتكافئة والكافية. والواقع أن اشتراط الحماية الكافية لا يتطلب أن تكون لدى الدولتين المشاركتين في نقل البيانات نظاما من القواعد المتماثلة، ولكنها تقتضي فقط أن يكون لكليهما تشريعات قابلة للتطبيق وفعالة في مجال حماية البيانات. أنظر:

Marios Koutsias, « The international reach of European Union data protection law and the United States: is international trade in 'safe harbor' ? », 2012, 18 (2), International Trade Law and Regulation, p. 35.

[3] Graham Pearce, Nicolas Platten, « Orchestrating Transatlantic Approaches to Personal Data Protection: a European Perspective », 1998-

و في حقيقة الأمر حتى وإن بقيت القواعد متشابهة تقريبا في بلدان الاتحاد الأوروبي، فإن المواجهة الأبدية على الخط الأطلسي تبقى مستمرة. مقاربتي الكومنلوث " *common law*" الأمريكي و القانون المدني الأوروبي غير متوافقتين حاليا، حيث يتطلب نقل البيانات على الخط الأطلسي وضع قواعد مشتركة تلبي في الوقت نفسه المتطلبات الأمنية و الأهداف التي يطمح إليها الفاعلون التجاريون المعنيون.

ثانيا: بناء الهوية و السمعة الرقمية.

منذ صدور الحكم Niemietz عن المحكمة الأوروبية لحقوق الانسان[1] ينبغي أن يقصد بالجانب الاجتماعي لحماية الحياة الخاصة على أنه "حق الفرد في إقامة و تطوير علاقات مع أشباهه". في المجال الرقمي تجد هذه الاستقلالية الشخصية امتدادها في امكانية نسخ و تحكّم الشخص في هويته(1). في هذا الاتجاه يصاحبها الحق لكل فرد في "معرفة ما نعرفه عنه"[2] لتوفير حماية أفضل لبناء سمعته على الانترنت(2).

1999, 22 Fordham International Law Journal, p. 2024-2027; R. Jones, « Extraterritoriality and international transfers under the draft Regulation », 2012, 12 (3), PDP 6; Christopher Kuner, « Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future », Tilt Law & Technology Working Paper Series 1, oct. 2010, n° 16; Alexander Zinser, « International Data Tranfer out of the European Union: the adequate level of data protection according to article 25 of the European Data Protection Directive", 2002-2003, 21 J Marshall, J Computer & Info, L, p. 547-548.

[1] CEDH, Niemietz c/ Allemagne, 16 déc. 1992, n°13710/88.

[2] Hélène Hurpy, « Fonction de l'autonomie personnelle et protection des droits de la personne humaine dans les jurisprudences constitutionnelles et européennes », thèse, Univ. Aix-en-Provence, 27 juin 2013.

1- الهوية الرقمية.

في بيئة تمتد فيها الإنترنت إلى الشبكات المحمولة و الأرضية، حيث تتضاعف وتتنوع أشكال وسائل الاتصال باستمرار، حيث الترابط بين الدخول والطرفيّة والموقع في نمو مستمر، يصبح الإنسان النقطة الرئيسية لتقارب الشبكات والخدمات[1]. و من المفارقات أنه أصبح من الصعب البقاء متسترا على شبكة الأنترنت في حين يكون سهلا الكشف عن هويته من طرف محركات البحث، ندرك إذن أن عدم الظهور في نتائج بحث غوغل يمثل انعداما للوجود في عالم الإنترنت، بل و ربما قد يثير ذلك بعض الريبة للبعض.

تثير اشكالية الهوية الرقمية تساؤلات عديدة اجتماعية وأخلاقية وقانونية وتكنولوجية[2]. إن الفرد عند تحديد مكانته في المجتمع، يلجأ إلى آلية تحديد الهوية[3]. حيث يحدد أولا هويته الذاتية وهذا يعني ماهيته الثقافية والفكرية. بعد ذلك يخضع إلى هويته الموضوعية التي ينقلها جسده. يختار إذن بحرية الأولى، ولكن تفرض عليه الثانية. في الواقع الرقمي يغطي التستر الهوية الذاتية، في حين تتحول الهوية الموضوعية إلى مخزن للبيانات يوفّر للشخص خيارات لا محدودة من الشاشات بين الحياة الحقيقية والحياة الافتراضية[4].

إنّ القواعد القانونية التي تحكم هذه الظاهرة الجديدة المتمثلة في الهوية الرقمية لا تزال غير واضحة. تماما كما هو الحال في أنه ليس من السهل دائما

---

[1] Daniel Kaplan, « L’identité numérique: esquisse d’un programme de travail », Fondation Internet Nouvelle Génération, 28 mai 2001.

[2] Jean-Pierre Ancel, « Protection de la personne: image et vie privée », Gaz. Pal., 2-6 sept. 1994.

[3] "إن هويتي هي التي تعني أنني لاأشبه أي شخص آخر" أمين معلوف.

[4] Jeoffrey Sabbah, « L'appréhension de l'identité sur Internet », RLDI, n° 101, févr. 2014, p. 99-103.

على المستوى القانوني تحديد الأعمال التي يقوم بها الأفراد على شبكة الإنترنت، و تبقى أيضا المهمة معقدة في تأطير الممارسات المتعلقة بالبيانات التقنية التي تسمح برقمنة سمات الفرد من الأصل[1].

البيانات التي تنطوي عليها عملية الرقمنة هي البيانات التقنية وبيانات الحاسوب المحضة، غير المفهومة لمعظم المستخدمين، والتي تتميز بكونها خارج نطاق رقابة الفرد المتصل بالانترنت، الذي يريد بكل بساطة الاتصال بالانترنت وليس إظهار معلوماته التي سوف تعرضها هويته الرقمية أمام أعين المستخدمين الآخرين. وبالتالي فإن هذه البيانات مسؤولة عن بناء الهوية الموضوعية للشخص. يمكن تمييز ثلاث فئات من البيانات التقنية. يتعلق الأمر في البداية بالبيانات التي تربط الفرد في العالم الحقيقي بالعالم الافتراضي من خلال اتصال آلة الحاسوب بالإنترنت وتعريفها في الشبكة (مثل عنوان بروتوكول الإنترنت IP address ، وعنوان MAC أو ما يسمى بالعنوان الفيزيائي Physical Address، رقم الهوية الدولية للأجهزة المتنقلة IMEI). ثم هناك بيانات تمكّن المستخدم من تسجيل دخوله للوصول إلى أجزاء غير عامة من الشبكة: حساب البريد الإلكتروني، المدونة، الصفحة الشخصية، الخ. هذه البيانات التعريفية لا تحدد بأي شكل من الأشكال سمات الهوية الرقمية للشخص، لكنها تسمح فقط من التحقق من هويته (ما دامت السمات المتعلقة بهذه الهوية تسمح بتحديد الشخص بطريقة وحيدة لا لبس فيها). هذه الفئة تشمل ما يصفه بعض الفقهاء بأنها "الهوية-الجسم"، و المتمثلة في البيانات البيومترية والوثائق

[1] Philippe Mouron, « Internet et identité virtuelle des personnes », RRJ 2008, n° 124, p. 2409.

الإلكترونية المؤمنة التي تصدرها الدول[1]. وأخيرا تدخل في الفئة الأخيرة بيانات الاتصال بالانترنت التي تتشكل من آثار، وهي بصمات يتركها الأفراد عند تصفحهم للشبكة[2]. لا تشمل فقط هذه البصمات عناوين IP (بصفة خاصة عنوان مرسل الرسالة و متلقيها)، و العناوين المرتبطة بتاريخ ووقت الاتصال بالانترنت، والمعلومات المحددة لنوع الاستخدام (الوصول إلى شبكة الإنترنت أو البريد الإلكتروني)، ولكن أيضا التطبيق نفسه (عنوان URL للموقع الذي يريد المستخدم زيارته). يتم تخزين هذه البيانات في ملفات تسمى "ملفات السجل" توجد في أجهزة الكمبيوتر الخاصة بمقدمي خدمة الانترنت أو الخوادم. وتقع أيضا في هذه الفئة ملفات تعريف الارتباط (الكوكيز cookies) و سجل التصفح historique de navigation التي تسمح من جهة لمستخدم الإنترنت من التحرك بسهولة بين مختلف الخدمات الرقمية، ومراقبة أنشطته من أجل مكافحة أفضل للجريمة المعلوماتية من جهة أخرى، في الوقت الذي يلتزم فيه مقدمو خدمات الإنترنت بالاحتفاظ ببيانات الاتصال لفترة يحددها القانون[3].

---

[1] "L'identité-corps": Eric Freyssinet, Guillaume Desgens-Pasanau, « L'identité à l'ère du numérique », D., Paris, 2009.

[2] بيانات الاتصال هي جميع البيانات "المتعلقة بالتقنيات المستخدمة على الإنترنت لإقامة اتصال بين أجهزة الكمبيوتر البعيدة (بروتوكول TCP/IP) واستخدام الشبكة من قبل الفرد ؛ فإنها تتعلق من جهة بعناوين أجهزة الشبكة، وتسمى عناوين بوتوكول الانترنت (IP)، ولا سيما الخاصة بمرسل الرسالة والمتلقي، وهي عناوين ترتبط بتاريخ ووقت الاتصال، المعلومات التقنية التي تميّز كل استخدام (الدخول إلى موقع أو بريد إلكتروني)، ومن جهة أخرى الموقع الذي يريد المستخدم زيارته أو الرسالة نفسها "، أنظر:

CE, Internet et les réseaux numériques: Doc. fr. 1998.

[3] تنص المادة 11 من قانون 09-04 الصادر بتاريخ 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها على التزام حفظ مقدمي الخدمة للبيانات لمدة سنة واحدة ابتداءا من تاريخ التسجيل.

ضمن هذه البيانات التقنية المختلفة: ستكون "الهوية–الجسم" من اختصاص السلطة الحصرية للدول، وبما أنها تستخدم عناصر بيومترية فإنها تخضع لمراقبة مركزية. ومن أمثلتها بطاقة الهوية الوطنية الرقمية وجواز السفر البيومتري أو رخصة السياقة الرقمية. والضمانات المرتبطة بها في تحديد هوية الشخص هي الأقوى، كما هو الحال بالنسبة للوثائق التقليدية: بطاقة الهوية وجواز السفر، إلخ، لأن الأمر يتعلق بتدعيم و اعادة التأهيل وفقا لقواعد العالم الرقمي للعناصر ذات الصلة بالحالة المدنية (الاسم واللقب وتاريخ ومكان الميلاد، الخ) أو بالصفات الفيزيولوجية و التشريحية للأشخاص (بصمات الأصابع، التعرف على الوجه، الخ). ويتم منح هذا النوع من الهوية حاليا في العديد من البلدان في العالم من بينها الجزائر حيث تم الشروع في تداول جواز السفر الوطني البيومتري الالكتروني[1] ابتداءا من تاريخ 05 جانفي 2012[2]. وعادة ما يأخذ شكل بطاقة أو دفتر يحتوي على شريحة رقمية[3].

وراء هذا التنوع من الهويات الرقمية باتت مسألة الهوية الحقيقية للشخص أكثر أهمية من أي وقت مضى. حيث نتساءل بشكل تلقائي من هو الشخص الذي يختبئ وراء عنوان البريد الإلكتروني، أو الصورة الرمزية او افاتار (Avatar) أو الروبوت (الأداة "الذكية"."smart" item"). ما هي الوسائل لتحديد هويته مع العلم أن الهويات يمكن أن تكون "قوية" (كاملة أو قادرة على إدارة وتوقيع

---

[1] قرار مؤرّخ في أوّل صفر عام 1433 الموافق 26 ديسمبر سنة 2011، يحدد المواصفات التقنية لجواز السفر الوطني البيومتري الإلكتروني.

[2] قرار مؤرّخ في أوّل صفر عام 1433 ا لموافق 26 ديسمبر سنة2011، يحدد تاريخ بداية تداول جواز السفر الوطني البيومتري الإلكتروني.

[3] المادة 6 من القرار المحدد للمواصفات التقنية لجواز السفر الوطني البيومتري الإلكتروني:

"يكون جواز السفر البيومتري الإلكتروني في شكل دفتر من 14 ورقة مزدوجة.وترقم صفحاته من 3 إلى 28. ولا تحتوي الصفحتان الأولى والثانية على رقم".

المعاملات) أو "ضعيفة" (مبسطة، بدون أي قدرة حقيقية على التصرف) و أن عدم التفاعل الجسدي في مجال الاتصالات عبر الشبكة يشجع ويسهل اللجوء إلى هويات مستعارة، بما في ذلك استخدام أسماء وهمية؟ إلى أي درجة يمكن لنا أن ننسب له أعمالا تثير مسؤوليته؟ في النهاية هل من الممكن رفع دعوى قضائية ضد صورة رمزية، باعتبارها إسقاطا لشخص معين، و الذي يتمتع بشخصية طبيعية حقيقية؟ بناء الهوية الرقمية، ودرجة استقلال مختلف عناصرها بالنسبة لصاحبها، أو قيمتها الثبوتية في حالة ابرام المعاملات، لا تزال مجالات لم يطرق بابها بعد[1].

في الجزائر هناك سوى بعض البيانات التقنية موضوعا للحماية القانونية وهي بيانات متعلقة بالحالة المدنية للشخص (اللقب، الاسم، العنوان، إلخ)، أما بيانات تحديد الهوية الرقمية مثل عنوان البريد الإلكتروني أو الاسم المستعار الافتراضي فإنها تبقى خارج نطاق تطبيق النصوص، بسبب أن الاعتراف بها باعتبارها بيانات شخصية ليس واضحا. للأسف ترك هذا فراغا قانونيا بشأن بعض الممارسات مثل التصيد الإلكتروني « phishing »[2] أو إنتحال عنوان بروتوكول الإنترنت (« *IP spoofing* ») والتي لا يمكن بالتالي ردعها. إن الترسانة القمعية القائمة في الواقع مقيّدة جدا، حيث تشمل إنتحال الهوية المدنية

---

[1] V. D. Kaplan, « L'identité numérique. Problématique et esquisse d'un programme de travail », Fondation Internet Nouvelle Génération, 28 mai 2001.

[2] ويسمى أيضاً الاحتيال الإلكتروني والاستدراج الإلكتروني واللصوصية. ويعني قيام شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني بدعوى أنه من شركة نظامية ليرتبط متلقي الرسالة بهذه الشركة، ويطلب الحصول منه على بعض المعلومات الشخصية مثل تفاصيل الحسابات المصرفية، وكلمات المرور، وتفاصيل بطاقة الائتمان... ليقوم باستخدامها للدخول إلى الحسابات المصرفية عبر الإنترنت، أو إلى مواقع الشركات التي تطلب البيانات الشخصية للسماح بالدخول إلى الموقع.

فقط(الركن المادي) للإفلات من المتابعة الجزائية أو الحصول على مزية غير مستحقة(عنصر القصد). من الناحية التقنية فإن النصوص الحالية المطبقة في الجزائر سواء تعلق الأمر بقانون العقوبات أو القوانين الخاصة لا تتطابق مع أشكال الانتحال الجديدة الناتجة عن الاتصالات الرقمية. وهكذا فإن إنشاء حساب شخصي على موقع فيسبوك باسم الغير لا يدخل في نطاق تطبيق المادة 249 من قانون العقوبات[1]، لذا فإنه لا يمكن إدانة منتحلي الهوية على الإنترنت في غياب النصوص المجرمة (الركن الشرعي).

لسد هذا الفراغ القانوني تم في فرنسا اعتماد القانون رقم 2011-267 المؤرخ في 14 مارس 2011 بشأن التوجيه والتخطيط لأداء الأمن الداخلي[2] حيث أصبحت المادة 226-4-1 من قانون العقوبات تجرم " انتحال هوية الغير أو استعمال بيانات مهما كانت طبيعتها تسمح بالتعرف عليه بهدف الاخلال بهدوئه، أو هدوء الغير، أو المساس بشرفه أو إعتباره". رحّب الفقه بهذا التطور التشريعي الذي يسمح أخيرا بردع منتحلي الهوية الذين لم يعد هدفهم الوحيد التهرب من العدالة أو الحصول على مزية اقتصادية غير مستحقة، أو – كما اعتبرته الجمعية الوطنية الفرنسية في القراءة الأولى – "المساس بالسلامة البدنية

---

[1] "كل من انتحل إسم الغير في ظروف أدت إلى قيد حكم في صحيفة السوابق القضائية لهذا الغير أو كان من الجائز أن تؤدى إلى ذلك يعاقب بالحبس من ستة أشهر إلى خمس سنوات بدون إخلال بإتحاذ الإجراءات ضده بشأن جناية تزوير إذا اقتضى الحال ذلك. و يعاقب بالعقوبة ذاتها كلمن تسبب عمدا في قيد حكم في صفيحة السوابق القضائية لغير المتهم و ذلك بإدلاء بأقوال كاذبة متعلقة بالحالة المدنية لهذا المتهم".

[2] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (loi LOPPSI).

أو النفسية للأشخاص " ولكن الاضرار بالضحية مساسا بشخصيتها أو بحياتها الخاصة[1].

متى إذن يتم الاعتراف بالحق في حماية الهوية الرقمية في الجزائر؟

2- السمعة الرقمية.

ظهر لأول مرة مصطلح "السمعة الرقمية" في عام 2000 في مقال بعنوان « *E-reputation: the role of mission and vision statement in positionning strategy* »[2]

يعرّف الكاتبان المهتمان بصورة العلامة التجارية للشركات، السمعة باعتبارها "البناء الجماعي و أنها مصطلح يشير الى صورة الشركة من وجهة نظر المساهمين" والسمعة الرقمية على أنها " عنصر السمعة الذي ينشأ حصريا من المتصلين الرقميين ".

وبالنظر إلى صعوبة التحكم في السمعة الرقمية، تظهر أولى الاشكالات القانونية لتؤكد الطابع الأساسي للمسائل المتعلقة بصورة الأشخاص والكيانات في الشبكة، من خلال المساس بالسمعة الرقمية الذي يتجسد في جرائم الصحافة لا سيما القذف، الاهانة و السب.

كل يوم يتم مشاركة الملايين من الصور الشخصية ومقاطع الفيديو على شبكة الإنترنت. في كثير من الحالات يتم نشر هذه البيانات الشخصية من دون موافقة مسبقة من الشخص المعني، أو حتى دون معرفته. بالنسبة للأفراد قد يكون للنشر الهائل للمعلومات الشخصية على الانترنت عواقب سلبية كبيرة على الحياة

---

[1] Romain Gola, « Usurpation de l'identité sur l'Internet: aspects de droit pénal comparé », RLDI 2009/55, n° 1839, p. 67.

[2] Rosa Chun, Gary Davies, « E-reputation: the role of mission and vision statement in positionning strategy », Journal of Brand Management, Vol. 8, n°. 4 et 5, mai 2001, p. 19.

الشخصية والمهنية والاجتماعية للأشخاص، خاصة بسبب بقاء هذه البيانات في مواقع تعاونية مختلفة.

في حين تشير الدراسات أنه وبصفة خاصة في المجال المهني، أصبح شائعا البحث في الإنترنت عن معلومات تخص شريك مهني محتمل (الموظف، رب العمل، الشريك، الخ)، وللحد من التجاوزات تدخل المشرع في بعض الدول لتنظيم مثل هذه الممارسات. وهكذا جاء مشروع قانون ألماني مؤرخ في 25 أوت 2010 بشأن حماية البيانات الشخصية للعمال ويهدف بشكل خاص إلى منع أرباب العمل من الاطلاع على الحسابات الشخصية لطالبي العمل على الفيسبوك[1]. في فرنسا لا وجود إلا للمادة L. 1132-1 من قانون العمل و التي تمنع من أن تؤدي المعلومات عن الأصل أو الجنس، والأخلاق، والتوجه الجنسي أو العمر أو الحالة العائلية، الميزات الوراثية، العرق أو الرأي السياسي أو الدين أو المظهر الجسدي، اسم العائلة، مكان الإقامة أو الحالة الصحية إلى الاضرار بطالب العمل عند التوظيف أين يتحفظ صاحب العمل المرتقب على إحدى المعلومات المذكورة أعلاه في إطار ممارسته لإلتزامه بالتعرف عليهم. وبالمقابل أصبح من الشائع أن تقوم شركات التوظيف بالتوقيع على مواثيق يتعهدون من خلالها على وجه الخصوص باستخدام الشبكات الاجتماعية المهنية وليس الشخصية، وعدم استخدام محركات البحث والشبكات الاجتماعية للتحقيق بشأن موظفهم المستقبلي، وتوعية مستخدمي ومسيّري هذه المواقع بشأن هذه القضايا. وبصرف النظر عن الاطار المهني، فإن تحديّات حماية السمعة الرقمية أبعد من مجرد تسيّير لصورة حسنة على الإنترنت. بالنسبة للأفراد، بما في ذلك الشخصيات العامة، يتعلق الأمر بحماية الشرف والاعتبار.

---

[1] Bundesdatenschutzgesetz, Bundesdatenschutzgesetz in der Fassung der Bekanntmachung, 14 janv. 2003 (BGBl. IS. 66).

ولكن حتى لو كان الحق في الصورة من الحقوق المعترف بها عموما للجميع، أصبح من الصعب تجسيده على نحو متزايد أمام الممارسات التي طوّرها مستخدمو الانترنت. تقليديا فإن الحق في الصورة يعد شكلا من أشكال الحق في ملكية سمة شخصية. أي وحدها الموافقة الصريحة من الشخص المعني تسمح بتجريده من حقه في احتكار صورته. لكن أمام الاستخدام المكثف لأدوات الاتصال الإلكترونية الذي أدى إلى تطور المقاربة المتعلقة بقيمة الصورة في سياق حماية الحياة الخاصة للأشخاص. على الأقل فيما يتعلق بأعمال النشر، فليس من السهل ضمان حماية الصورة في زمن الصورة الملتقطة ذاتيا (السيلفيات *selfies*) و التي يتم تداولها في كل مكان في الشبكة.

إن شرط الموافقة أصبح أقل تقييدا فيما يتعلق بالصورة الملتقطة ذاتيا لأنه من البديهي أنها نشرت من قبل الأشخاص المعنيين أنفسهم، يمكن لنا منطقيا استنتاج أن الرضا مفترض. في هذا السياق إذا قمنا بتطبيق نفس التفرقة التي تبناها فرانسوا ريقو François Rigaux بالنسبة للحق في الحياة الخاصة على الحق في الصورة – "في إطار الأشكال المتعددة للمساس بالشخصية يمكن التمييز بين التي تكشف حقائق خاصة يحميها الحق في السرية و تشويه الصورة التي أراد الفرد تقديمها عن نفسه للجهات الفاعلة الاجتماعية الأخرى "[1] نرى أن الجانب الأول المتعلق بالسرية يفقد أهميته بالمقارنة مع انتشار صورة في الشبكات الرقمية. نفس الشيئ بالنسبة لاستخدام صورة الغير، وحتى لو كان رضا الشخص قائما دائما (ولا سيما فيما يتعلق بالاستخدام التجاري)، يتم الانتقال تدريجيا إلى نظام تكون فيه مراقبة المشروعية في نشر صورة الشخص مبنيا على تقدير المساس أساسا على قاعدة الخطأ أو الفعل الضار على الشبكة.

---

[1] François Rigaux, « La protection de la vie des autres biens de la personnalité », Bruylant-LGDJ, 1990, p. 275.

في نهاية المطاف فإن أفضل طريقة لتسيير السمعة الرقمية هو تبني الآليات التي تعرضها الرقمنة، مع العمل على مراقبة الطريقة التي يتم بها استخدام هذه الآليات من قبل الآخرين. لبناء فعّال للهوية الرقمية الخاصة بهم و في نفس الوقت تحسين و تطوير علاقاتهم، يجب على الأفراد والشركات أن يكونوا قادرين على الحفاظ على مستوى معين من الرقابة على ما يتم نقله إلى علم الجمهور.

ثالثا: الحق في التستر.

للبقاء متسترا إلى حد ما في الفضاء الرقمي، يجب أن يكون الفرد حرا في اختيار ما يتعلق به، الوقت والظروف والمدى التي يتم فيها مشاركة المواقف والمعتقدات والسلوكيات والآراء مع الآخرين أو إخفائها عنهم. من هذا المنظور ينضوي التستر تحت نظرية التحكم في استخدام البيانات الشخصية التي سيتم التطرق إليها لاحقا. وبذلك فهو يشكل جزءا من فكرة حماية الحياة الخاصة (1). سوف نلاحظ في الممارسة العملية إلى أي حد يتم ضمان هذا الحق لصالح مقدمي المحتوى الرقمي وإلى أي مدى يمكن أن يمارس من خلال استخدام اسم مستعار (2).

1- الحق في التستر كعنصر من عناصر الحق في الحياة خاصة وحرية التعبير.

في غياب تعريف قانوني للتستر[1]، يمكن تعريفه على أنه "الحالة التي يكون عليها الشخص عندما لا تمنعه قاعدة قانونية في عدم التعريف بنفسه في علاقاته مع الآخرين "[2]. وبالتالي يمكن أن يفهم الحق في التستر باعتباره حرية عدم الكشف عن هويته في أنشطة الحياة اليومية، حتى تلك التي يترتب عنها آثار قانونية. هذا يعني عادة حرية الجميع في عدم وضع اسمه على صندوق بريد،

---

[1] فيما يتعلق بالتستر أنظر: Jean-Christophe Saint-Pau, « L'anonymat et le droit », thèse, Bordeaux IV, 1998.

[2] Pour Jean-Christophe Saint-Pau, op.cit. n° 10.

الاشتراك في خدمة القائمة الحمراء و عدم الظهور في دليل الهاتف، رفض الكشف عن هويته باستثناء الحالات التي ينص عليه القانون[1].

من خلال معالجة مسألة حماية الحياة الحياة الخاصة على الإنترنت، اعتبرت لجنة وزراء مجلس أوروبا أن "الوصول والاستخدام المتستر للخدمات (...) يشكل أفضل حماية للحياة الخاصة ".

يرى بعض الفقهاء أنه من غير المعقول اليوم سواء في البيئة الرقمية أو التقليدية، تجنب التعرف على الأفراد بشكل كامل[2]، فمن غير الشرعي وجود امكانية في أن يكون الحق في التستر حقا تاما في عدم الكشف عن الهوية. في هذا السياق يتعلق الأمر بنفس المبادئ التي تحكم الحق في حماية الهوية الرقمية لأنه في أحسن الأحوال مجرد نشاط منظم للبيانات المحددة للهوية بحيث لا تتحول ضد الأشخاص المعنية بها. من خلال هذه الضمانات يكون تستر الأشخاص محميا بمجرد احترام خيارهم في الحفاظ على هويتهم من أي تشويه.

إن النظرة الأكثر شيوعا عن التستر ولكن الأكثر تقييدا، يعتبر البعض الحق في التستر في السياق الرقمي على أنه "كل شخص طبيعي حرّ في استخدام هويته الرقمية، و أن له خاصة الحق في تشفير هذه الهوية لأغراض السرية والتستر"[3]. التستر على الإنترنت يقابله رفض الكشف عن هويته في الأماكن العامة. على وجه التحديد يتعلق الأمر إذن بـــ"التشويش" على هويته في الشبكة، سواء من خلال استخدام اسم مستعار، من خلال الاحتفاظ ببعض المعلومات، من خلال تعدد

---

[1] على سبيل المثال الزامية كتابة الهوية الاجتماعية كما جاء في نص المادة 453 ق.ع.

[2] و ذلك من اللحظة التي يقوم فيها مقدم الخدمة بالاحتفاظ بعنوان بروتوكول الانترنت IP للجهاز المستعمل في الاتصال بالانترنت.

[3] Groupe de travail TIC, « Déclaration des droits de l’homme numérique », Mairie d’Issy-les-Moulineaux, Livre blanc d’André Santini et d’Alain Bensoussan, 20 nov. 2000, p. 18.

عناوين البريد الإلكتروني المستخدمة أو عن طريق التصريح الكاذب[1]. ينطبق هذا المفهوم بوجه خاص على الشبكات الاجتماعية، حيث يمكن اعتباره بأنه "الحق في التصرف في خدمة للتواصل الاجتماعي تحت اسم مستعار دون الكشف عن هويته الحقيقية للمستخدمين الآخرين أو إلى جمهور أوسع "[2]. تفسيره بهذه الطريقة يظهر الحق في التستر كامتداد لحرية التعبير[3]. على هذا النحو و متى كانت حرية التعبير من بين الحريات المكفولة دستوريا بموجب القانون الأساسي الألماني، اعتبر القاضي الألماني الالتزام المفروض على الأفراد بالتعريف عن أنفسهم للتعبير عن آرائهم عبر منصات الانترنت، يخلق بشكل عام خطرا في إمكانية أن يقرر الشخص الامتناع عن التعبير عن رأيه خوفا من الانتقام أو من أي نتيجة سلبية أخرى، والذي يمكن أن يؤدي إلى آثار تتمخض عن رقابة ذاتية[4].

---

[1] Genevieve Bell, « Secret, lies & the possible perils of truthful technology », conférence prononcée dans le cadre duprogramme Lift de la Fing, 2008.

[2] تقرير فريق العمل الدولي المعني بحماية البيانات الشخصية في مجال الاتصالات، أنظر:
« Report and guidance on privacy in social networks services » (« Rome memorandum »), 4 mars 2008, 675.36.5, http://www.datenschutz-berlin.de/content/europa- international/international-working-group-on-data-protection-intelecommunications-iwgdpt/working-papers- and-common-positions-adopted-by-the-working-group.

[3] أنظر في هذا الاتجاه:
Arista Records c/ Doe 3, Docket n° 09-0905-cv, 29 avr. 2010, U.S. Court of Appeals, 2d Circuit.
ينوه القاضي الأمريكي في هذا القرار بأن حرية التعبير على الإنترنت تتمتع بأعلى مستوى من الحماية بموجب البند الأول من الدستور الأمريكي، وأن إمكانية التستر على الإنترنت، التي هي جزء من نفس هذه الحرية أي حرية التعبير، يجب حمايتها.

[4] Tribunal fédéral allemand, 15 déc. 1983, Volksählungsgesetz, BverfGE 65, 1, 41. 38. V. D. Kaplan, « Informatique, libertés, identités », FYP, 2010, p. 69. 90.

ولكن أبعد من فكرة القدرة على التصرف دون الكشف عن هويته الحقيقية، يتجسد الحق في التستر أيضا من خلال الحق في معارضة التحقيق والكشف عن هويته المدنية، المادية والاقتصادية[1]. في هذا السياق فإن انتهاك هذا الحق قد يفتح الباب للمطالبة بالتعويض على أساس المادة 9 من القانون المدني.

دول أخرى مثل اليابان اختارت الاتجاه المعاكس بحظر استخدام نظام متصفح TOR وهو برنامج التصفح المتستر على الإنترنت، تحت ذريعة سوء الاستخدام. في الصين وبموجب قرار مؤرخ 28 ديسمبر 2012 اعتمد المؤتمر الوطني لنواب الشعب الصيني التدابير الجديدة التي تسري على كافة التراب الوطني التي تلزم مستخدمي الإنترنت بالكشف عن هويتهم الحقيقية ورقم الهاتف النقال الخاص بهم لمقدمي خدمات الإنترنت[2].

في هذا السياق يبدو من الضروري الاشارة إلى أنه على خلاف الدول الأوروبية، فإنه في الولايات المتحدة الأمريكية لا يعتبر كشف الهوية مبدأً بينما

---

[1] وبالتالي هناك انتهاك لحرمة الحياة الخاصة بإجراء تحقيقات لجمع المعلومات عن هوية الشخص

(Cass. 1re civ., 13 févr. 1985: JCP G 1985, II, 20467, 2e esp. note R. Lindon),

وعنوانه، وحالته الثقافية والمهنية، وشروط شغله لمسكنه

(Cass. 1re civ., 19 déc. 1995: D. 1997, p. 158, note J. Ravanas. – Cass. 1re civ., 6 mars 1996: D. 1997, p. 7, note J. Ravanas ; Cass. 1re civ., 30 mai 2000, n° 98-14.610: JurisData n° 2000-002307 ; Bull. civ. 2000, I, n° 167 ; JCP G 2002, II, note B. Montels ; RTD civ. 2000, p. 801, note J. Hauser). هذا التصور يأتي في نفس سياق الاجتهاد الأوروبي (V. p. ex., Schlumpf c/ Suisse, 8 janv. 2009, § 100) الذي يحدد على أن مفهوم الحياة الخاصة يمكن أن يشمل أحيانا جوانب من الهوية المدنية والاجتماعية للفرد. (CEDH, n° 53176/99, Mikulic c/ Croatie, § 53, 2002-I)

[2] ترجمة القرار بالنجليزية متوفرة على العنوان التالي :

http://blog.feichangdao.com/2012/12/translation-decisionregarding.html.

يتلقى التستر حماية قانونية قوية. حيث أن كل محاولات إخضاع الوسطاء التقنيين لالتزام حيازة البيانات المحددة لهوية المستخدمين قد باءت بالفشل حتى الآن[1].

النصوص المعمول بها في هذا المجال: البند الرابع على المستوى الدستوري وقانون الاتصالات الإلكترونية عام 1986 على المستوى القانوني.

وكذلك الحال في كندا أين أكدت المحكمة العليا[2] في قرارها الأخير أن التستر على الإنترنت حق مكفول، وأنه على قوات الأمن حيازة إذن قضائي لمطالبة مقدمي خدمة الإنترنت بمعلومات عن بعض الزبائن.

وأخيرا ووفقا للمادة 6 من توجيه المفوضية الأوروبية EC/58/2002 فإنه " يجب حذف أو تغفيل البيانات المتعلقة بنشاط المشتركين والمستخدمين، المعالجة والمخّزنة من طرف مقدم لخدمة شبكة عامة للاتصالات أو لخدمة اتصالات الكترونية متاحة للجمهور، عندما لا تعود لازمة للاتصال (...) ".

تبنت فرنسا هذه الآلية من خلال المادة 34-1 من قانون البريد والاتصالات الالكترونية حيث تنص "على متعاملي الاتصالات الإلكترونية، وخاصة تلك التي يكون نشاطها تقديم خدمات الاتصال للجمهور على الانترنت، حذف أو تغفيل أي بيان متعلق بنشاط الشبكة ". وبالتالي فمن المسلم به أنه لا يتم حذف البيانات تلقائيا، ولكن يتم تغفيلها.

بغض النظر عن المخاطر المرتبطة بالتستر هناك عدة استثناءات لحذف أو اغفال البيانات. على سبيل المثال يمكن أن يحتفظ بهذه البيانات لمدة سنة وارسالها للغير لأسباب أمنية. وأخيرا فيما يتعلق بتعريف الأشخاص من خلال العمليات

---

[1] عدة مشاريع قوانين في هذا السياق في 1999 ل SAFETY Act إلا أنه لم يتم المصادقة عليها.

[2] R. c. Spencer, n° 2014 CSC 43, 13 juin 2014, adresse: http://scc-csc.lexum.com/scc-csc/scccsc/fr/item/14233/index.do?r=AAAAAQAIYW5vbnltYXQAAAAAAQ.

عبر الإنترنت التي تتطلب مصادقة (الخدمات الإلكترونية، والحكومة الإلكترونية)، يلاحظ الفقه أن الحق في التستر الحقيقي يتجسد في "الفصل بين تخزين بيانات الهوية وإصدار الشهادات الإلكترونية "، وأنه على هذا النحو" وجب تكريسه كحق أساسي "[1].

2- حق محرري المحتوى الرقمي في التستر.

منذ اعتماد القانون رقم 575-2004 المؤرخ في 21 جوان 2004 بشأن الثقة في الاقتصاد الرقمي[2]، أصبح أصحاب المدونات وكذا الناشرين الهواة للمواقع الإلكترونية يعتمدون على شكل معين من حماية الهوية التي تسمح لهم بنشر أفكارهم تحت غطاء التستر – على الأقل في نظر الجمهور.

في هذا السياق فإن استخدام اسم مستعار هو بمثابة حل وسط بين احترام التستر والتزام التعريف بالهوية. إضفاء الطابع الديمقراطي على شبكة الإنترنت أدى إلى تكثيف استعمال الأسماء المستعارة: في البداية كان الاسم المستعار على شكل تسجيل للدخول("log-in")، ثم تطور مفهومه وأصبح مرتبطا ارتباطا وثيقا بالإنترنت[3]، وتحول إلى اسم مستخدم مشخصن بشكل غير محدود. أصبح الاسم المستعار الطريقة الأمثل بالنسبة للأفراد لتجنب التنميط والاستهداف بتقنيات التسويق المختلفة. أدى تنوع التطبيقات المستخدمة على الإنترنت إلى الاستبدال الجزئي للاسم المستعار بالمعرّف (كما يتضح من خلال المصطلحات المستخدمة

---

[1] Louise MERZEAU, Michel ARNAUD, « Traçabilité et réseaux », Hermès, n° 53, avr. 2009.

[2] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

[3] Guillaume Desgens-Pasanau, Eric Freyssinet, « L'identité à l'ère du numérique », 2009, Dalloz, p. 56.

من طرف العديد من خوادم البريد الإلكتروني أو منتديات النقاش)، لكن حاليا تعتمد المحافظة على أمن التعريف بالهوية أساسا على كلمة مرور أو رقم سرّي.

على المستوى الأوروبي كانت هيئة حماية البيانات G29 (التي تجمع بين سلطات حماية البيانات في دول الاتحاد الأوروبي) أول من اهتم باستخدام الاسم المستعار منذ سنة 1997، في بداية الأمر في سياق المدونات وعملية التعريف بالهوية لدى مقدمي خدمات الإنترنت[1]. وفي وقت لاحق أصدرت لجنة وزراء مجلس أوروبا عدة توصيات متعلقة بالشبكات الاجتماعية، عالجت بعضها الحق في استخدام اسم مستعار. في هذا الاطار أقرّت أن "ضمان الحق في استخدام اسم مستعار بالنظر إلى حرية التعبير والحق في الاتصال والحصول على المعلومات والأفكار، والحق في احترام الحياة الخاصة "[2]. ومع ذلك أكد مجلس أوروبا أن ضمان الحق في الاسم المستعار "لا يمنع [...]السلطات المخولة قانونا في الحصول على الهوية الحقيقية للمستخدم عند الضرورة، شريطة الالتزام بالضمانات القانونية المناسبة التي تكفل احترام حقوق الإنسان والحريات الأساسية ". دون تمتعه بقيمة مطلقة يظهر الاسم المستعار كوسيلة كاملة للحفاظ على الحقوق التي تكفلها الاتفاقية الاوروبية لحقوق الانسان والحريات الاساسية[3]. وعلى الرغم من أنه ليس لهذه التوصيات قوة قانونية ملزمة، إلا " أنها مثالية تعتمد عليها محكمة حقوق الإنسان الأوروبية من أجل تطوير اجتهاداتها "[4].

---

[1] Groupe de travail « Article 29 », Recommandation 3/97, L'anonymat sur Internet, WP 6, 3 déc. 1997, p. 9.

[2] Cons. E., Comité des ministres, Rec. du Comité des Ministres aux Etats membres sur la protection des
droits de l'homme dans le cadre des services de réseaux sociaux, CM/rec(2012)4, 4 avril 2012, p. 3

[3] CESDHLF: http://www.echr.coe.int/documents/convention_fra.pdf

[4] Ludovic Pailler, « Les réseaux sociaux sur internet et le droit au respect de la vie privée », Larcier, 2012, p. 61.

ولكن في الممارسة العملية تظهر العديد من الأمثلة أن استخدام اسم مستعار ضمن الأنشطة عبر الإنترنت لم يتحول بعد إلى حق مكتسب. على سبيل المثال و بمجرد إطلاقها سنة 2011، أرادت خدمة Google + حظر الحسابات المفتوحة تحت أسماء مستعارة. وبعد مناقشات حادة حول موضوع الهوية الرقمية قررت الخدمة أخيرا قبول تسجيل الحسابات الوهمية. من جانبه برّر فيسبوك سياسته المبنية على ثقافة الاسم الحقيقي بالقول أنها " تؤدي إلى قدر أكبر من مسؤولية المستخدمين و إلى بيئة أكثر أمانا "[1]. وهكذا عند التسجيل تطلب الشبكة الاجتماعية بعض المعلومات (الاسم واللقب وتاريخ الميلاد والجنس)، مع الاحتفاظ بالحق في تعليق الحساب في حالة عدم صحة البيانات المقدمة وعدم إثبات المستخدم لمطابقة المعلومات المقدمة بواسطة وثيقة هوية رسمية ممسوحة ضوئيا[2].

هذه السياسة المثيرة للجدل في بعض البلدان لا تخدم الحق في التستر، و بصفة خاصة في ألمانيا حيث أمرت سلطة حماية البيانات الشخصية في الولاية الإقليمية شليسفيغ هولشتاين، فيسبوك بتغيير سياسته في الخصوصية " pseudonymat " على أساس أنها مخالفة للتشريعات الألمانية والأوروبية المتعلقة بحماية حرية التعبير. تم الطعن في هذا القرار وفصلت المحكمة الإدارية لصالح فيسبوك. وفي منطوقها أشارت المحكمة الإدارية لولاية شليسفيغ هولشتاين أنه "وفقا للتوجيه الأوروبي المتعلق بحماية البيانات والقانون الألماني المتعلق

---

[1] Elliot Schrage, New York Times, « Facebook executive answers readers' questions », 12 mai 2010.

[2] بالفعل فإن المادة 4 من بيان الحقوق والمسؤوليات الخاص بفيسبوك تنص على أمان التسجيل والحساب بحيث يلتزم مستخدمو فيسبوك بتقديم أسماءهم ومعلوماتهم الحقيقية، ونحتاج إلى مساعدتك للمحافظة عليها على هذا النحو. وإليك بعض الالتزامات التي تتعهد بتقديمها لنا بشأن التسجيل والمحافظة على أمان حسابك.

بحماية البيانات، لا ينطبق القانون الألماني متى كان تسجيل ومعالجة البيانات الشخصية من طرف شركة تابعة تقع في بلد عضو في الاتحاد الأوروبي "[1].

وبالتالي فإن مسألة تطبيق المعايير الأوروبية في مجال التستر لا تزال مطروحة في الوقت الراهن، ما دامت تشريعات الدول مثل أيرلندا تفضل المتعاملين الذين يمارسون أنشطتهم على الإنترنت على مستعملي الخدمة التي يعرضها هؤلاء. تدريجيا تطورت المقاربة المنتهجة نحو نظام يتميّز بحماية أكبر للمستهلكين. في قرار صادر بتاريخ 29 يوليو 2015 عن سلطة مراقبة البيانات لمدينة هامبورغ الألمانية مماثل لقرار شليسفيغ هولشتاين، فصلت فيه لصالح مستخدم الإنترنت بأمر فيسبوك باعادة فتح حساب أحد مستخدميه والذي تم تعليق حسابه بحجة أن فيسبوك اعتبر أنه من الضروري المطالبة بالتحقق من هوية الشخص عن طريق إرسال وثائقه الرسمية.

وبالإضافة إلى ذلك ومن خلال مشروع اللائحة الأوروبية بشأن حماية البيانات الشخصية، يمكن أن يتمتع الاسم المستعار مستقبلا بنظام حماية موسّع. حيث ينص المشروع في مادته الرابعة على إدراج البيانات المستعارة و المشفرة في إطار تعريف البيانات الشخصية وبالتالي من المحتمل أن تتلقى الحماية المناسبة.

---

[1] أنظر:

http://www.schleswig-holstein.de/OVG/DE/Service/Presse/Pressemitteilungen/15022013VG_facebook_ anonym.html; facebook-s-fake-name-ban-backed-by-german-appeals-court ; B. Rooney, « The debate over online anonymity », Tech-Europe, Thje Wall Street Journal, 17 janv. 2013, adresse: http://blogs.wsj.com/techeurope/ 2013/01/17/the-debate-over-online-anonymity/.

حقوق الشخص على بياناته و إتصالاته الالكترونية.

في إطار المبادلات غير المادية ذات الطبيعة الخاصة، يتمتع مستخدمو الإنترنت بـــ"سلطة" معينة على ما يرسلونه. وتتجلى هذه السلطة في وجود حق في الحفاظ على سرية محتوى الرسائل الإلكترونية المتبادلة (أولا). و بشكل متوازي يمكن إتباع نفس المنطق بالنسبة للبيانات المتعلقة بالأشخاص. حيث يمكن للشخص السيطرة عل بياناته "الخاصة"، باعتبارها ملكا له (ثانيا). وكجزء من هذا الموضوع تنشأ إشكالية مهمة أيضا عن وجود حق في ملكية الشركات للبيانات السرية التي في حوزتها.

أولا: الحق في سرية الاتصالات الإلكترونية.

في حين أن التستر محظور في إطار المراسلات العامة المكتوبة و السمعية البصرية، إلا أنه لا يوجد أي نص يحظره في إطار المراسلات الخاصة ما دامت لا تهدف إلى الإضرار بالمرسل إليه (1). بينما تنشأ في المقابل إشكالية التشفير، والتي تبدو أنها تشكل الحل المناسب لضمان سرية الاتصالات الإلكترونية (2).

1- سرية الاتصالات الخاصة.

إذا رجعنا إلى التعاريف يعتبر سريا "ما يتم إبلاغه لشخص معين مع منعه من إفشائه إلى أي شخص كان. وما يتم تسليمه كتابة أو شفاهة تحت ختم السرية (في إطار الثقة والبوح)"[1]. المعلومة السرية تفترض بالضرورة وجود علاقة ثقة.

تنص المادة 10 من إتفاقية حقوق الإنسان و كذا العهد الدولي الخاص بالحقوق المدنية والسياسية الموقع في نيويورك في 19 ديسمبر 1966 على الحق في سرية المراسلات.

في الجزائر نصت المادة 39 من الدستور على ضمان سرّية المراسلات.

---

[1] Gérard Cornu, « Vocabulaire Capitant », coll. Quadrige, PUF, 2000, p. 192.

في فرنسا وخارج نطاق حرمة الحياة الخاصة، تسمح المادة 9 من القانون المدني أيضا بحماية الحق في حرمة المراسلات. وتشمل هذه الحماية أيضا الاتصالات الإلكترونية حيث يقّر قانون 10 يوليو 1991[1] مبدأ سرية المراسلات الخاصة التي تصدر عن الاتصالات عن بعد و يؤكد على حماية البريد الإلكتروني، باعتباره امتدادا لسرية البريد وحرمة الحياة الخاصة. كما أوصى مجلس الدولة بهذه الحماية في تقريره " الإنترنت والشبكات الرقمية " المعتمد من طرف الجمعية العامة بتاريخ 2 جويلية 1998 معتبرا أن "سرية المراسلات تضمن للمستخدم أن بياناته الشخصية الواردة فيها ستحظى بنفس الحماية التي يتمتع بها البريد العادي "[2].

في المجال الجزائي يعاقب قانون العقوبات الجزائري على انتهاك حرمة المراسلات في المواد 137 و303.

حدّد القاضي الأمريكي من خلال قرارات مختلفة، البيانات المتعلقة بالاتصالات التي تقع داخل أو خارج إطار حماية البند الرابع من الدستور. في الفئة الأولى نجد المحتويات الظاهرة للمتعامل (حيث أن هذا المتعامل يعتبر ناقلا للرسالة وليس متلقيا لها). لكن لا تتمتع بهذه الحماية المعلومات المتعلقة بحساب المستخدم، و البيانات الوصفية أو المحتوى المكشوف عنها طواعية إلى كيان معين (حيث يكون هذا الكيان هو المرسل إليه).

وفيما يتعلق بالحماية الفدرالية فإن القانون المطبق هو "قانون خصوصية الاتصالات الإلكترونية *Electronic Communications Privacy Act* "

---

[1] Loi n°91-646 du 10 juill. 1991 relative au secret des correspondances émises par la voie des communications électroniques, JO n° 162 du 13 juill. 1991.

[2] Conseil d'État, « Internet et les réseaux numériques », Doc. fr., 1998, p. 30.

الصادر سنة 1986، والذي يتضمن ثلاثة نصوص مختلفة. يتضمن أولا "قانون التنصت *Wiretap Act* " الذي يهتم بجمع البيانات المتعلقة بمحتوى الاتصالات. ويتضمن أيضا "قانون الاتصالات المخزنة *Stored Communications Act* "، المتعلق بالاتصالات المحتفظ بها الكترونيا و البيانات الوصفية والمعلومات المحاسبية[1].

وأخيرا فإنه يتضمن قانون سجلات القلم *Pen Register Act* " المتعلق بجمع البيانات الوصفية للاتصالات. ومن بين هذه النصوص فإن " قانون الاتصالات المخزنة " هو الأكثر ملاءمة من حيث سرية الاتصالات الهاتفية و الإلكترونية. القاعدة العامة إذن تتلخص في حظر إفشاء المعلومات المتعلقة بالاتصالات.

2- الحق في تشفير البيانات الرقمية لمنع الاعتراض غير القانوني.

يتيح التشفير حماية المعلومات الحساسة، سواء في إطار التخزين أو النقل، وعلى هذا النحو فإنه يشكل بالتالي جزءا هاما في أي نظام مؤمن للاتصالات الإلكترونية والتجارة الإلكترونية[2]، ويسمح بضمان السرية وصحة وسلامة البيانات. لا يدرك المعلومات المشفّرة إلا الأشخاص الذين يحوزون على مفتاح فك التشفير.

---

[1] د. مروة زين العابدين صالح، الحماية القانونية الدولية بين القانون الدولي الاتفاقي والقانون الوطني، ط1، مركز الدراسات العربية للنشر و التوزيع، 2016.

[2] Nathan Saper, « International Cryptography Regulation and the Global Information Economy », Northwestern Journal of Technology and Intellectual Property, automne 2013, vol. 11, issue 7, art. 5m adresse: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1205&context=njtip.

لذا فإن التشفير يشكل في نفس الوقت أداة أساسية لأمن البيانات في العصر الرقمي (التوقيع الالكتروني)، ولكن أيضا ضمانة لحرمة الحياة الخاصة وسرية المراسلات الالكترونية من خلال أنه يسمح من التأكد من هوية صاحب المراسلة من جهة، ومن سلامة هذه المراسلة من جهة أخرى، ذلك لأن البيانات المشفرة تتدفق عبر الشبكات دون قراءتها أو تغييرها أو تحويلها من طرف أشخاص غير مخولين. في الواقع وفي غياب الحلول في إطار التشفير غير المتماثل، يصبح مستخدمو الإنترنت غير قادرين على التواصل بشكل موثوق وليس في الاطار الخاص فقط ولكن أيضا في سياق العمليات المتعلقة بالتجارة الإلكترونية أو الخدمات المصرفية عبر الإنترنت على سبيل المثال. التشفير يسمح للأفراد التواصل عبر الانترنت بدون خوف من المراقبة الحكومية للمحتويات المتبادلة – سواء تعلق الأمر بنشطاء يناضلون من أجل احترام حقوق الإنسان في البلدان الاستبدادية، أو إرهابيين أو حتى متاجري المخدرات.

التشفير يسمح أخيرا بإنشاء واستخدام التوقيع الإلكتروني كشرط لإثبات الهوية[1]. وتستخدم الحكومات التشفير مثلها مثل الشركات والمؤسسات، لتأمين الوثائق ورسائل البريد الإلكتروني والمكالمات الهاتفية. يشكل بالتالي أفضل وسيلة للحفاظ على سرية المراسلات الرقمية وإن القضايا ذات الصلة بالاستعمال الحر لوسائل التشفير استخدام تشكل أهمية أساسية في سبيل احترام حقوق الأشخاص، سواء الطبيعية و أو الاعتبارية.

---

[1] Lyombe Eko, Natasha Tolstikova, « To Sign or Not to Sign on the Electronic Dotted Line: The United States, the Russian Federation, and International Electronic Signature Policy », 10 International Journal of Communications Law and Policy 1, 2 (2005), adresse: http://ijclp.net/old_website/10_2005/pdf/ijclp_05_10_2005.pdf. 26.

ومع ذلك فإن استخدامه تعيقه قيود تفرضها الحكومات سيتم تناولها لاحقا و تتمثل في: من جهة في تقييد استيراد وتصدير تكنولوجيات التشفير، وفي تنفيذ التزامات الكشف عن البيانات المشفرة في حالات معينة من جهة أخرى.

في الواقع فإن الكشف عن البيانات المرسلة في الشبكة لا يمس فقط بمبدأ سرية المراسلات والحياة الخاصة للأفراد، ولكن أيضا بالحياة التجارية بما أن الشركات و المؤسسات تستخدم بشكل مكثف تكنولوجيات التشفير، على سبيل المثال لإرسال معلومات سرية، بما في ذلك العناصر المتعلقة بالملكية الفكرية والأسرار التجارية، ولكن أيضا المراسلات التي تخص السر المهني (الرسائل المتبادلة بين ومع الأطباء، والمحامين، الخ). إن نظام التشفير القوي من النهاية إلى النهاية ("*end-to-end encryption*") متوفر على شبكة الإنترنت، سواء للاحتياجات المصرفية الإلكترونية أو التجارة الإلكترونية.

كما أنه يستخدم لتخزين وحفظ البيانات على دعائم مختلفة (الأقراص الصلبة، والرقائق، وغيرها). ويترتب على ذلك السؤال الذي يطرح نفسه عند السفر خارج الحدود مع أداة (الكمبيوتر المحمول أو الهاتف الذكي) تحتوي على برامج للتشفير أو بيانات مشفرة. في حين أن معظم الدول التي تفرض القيود على استيراد وتصدير تكنولوجيات التشفير تقّر بمفهوم الإعفاء للاستخدام الشخصي، وهذا ليس هو الحال في جميع البلدان. على سبيل المثال لادخال طرفية مشفرة إلى روسيا البيضاء، يجب على الفرد أن يحصل على ترخيص من وزير الشؤون الخارجية. في إيران يجب الحصول على إذن من المجلس الأعلى للثورة الثقافية. في أوكرانيا يتم الحصول على ترخيص من المصلحة الحكومية الخاصة للاتصالات.

في الوقت الحاضر الوسيلة الدولية الوحيدة التي تسمح بوضع دعامة مشتركة للقواعد التي تنطبق على واردات وصادرات التكنولوجيا ذات الاستخدام المزدوج

تتمثل فيما يعرف بترتيبات واسينارArrangement de Wassenaar الموقّعة في 12 ماي 1996. وبموجب المادة 87 من هذه الاتفاقية التي وقعتها حتى الآن 45 دولة، تم فرض التبادل الحر لتكنولوجيات التشفير المتناظر التي تتضمن مفتاح التشفير قد يصل طوله إلى 56 بايت والتشفير غير المتناظر مع مفتاح التشفير بطول يصل إلى 512 بايت. بالاضافة إلى ذلك تضمن النص استثناء الاستخدام الشخصي حتى يتسنى للأفراد العابرين لحدود البلدان الموقعة على الاتفاقية يمكن لهم أن يأخذوا معهم أجهزة التشفير التي يستخدمونها للأغراض الشخصية (المادة 85). وهذا التنويه مهم عندما ندرك أن معظم أجهزة الكمبيوتر والهواتف الذكية الموجودة في السوق حاليا تمتلك قدرات تشفير معينة. ومع ذلك يبقى هذا النص المؤسس غير ملزم للبلدان التي وقعته وبالتالي فإن تطبيقه يرجع إلى سلطتها التقديرية الكاملة.

ثانيا: الاعتراف المحدود بحق ملكية البيانات الرقمية في مواجهة ظاهرة الاتجار بالمعلومات.

تتعارض الاتجاهات المختلفة حول فكرة تملّك وتسليع المعلومات الأكثر حساسية على مستوى المجتمع العالمي: وهي البيانات الشخصية – أساس اقتصاد القرن الحادي والعشرين (1) لكن تطرح كذلك قضايا الملكية المتعلقة بالأصول غير الملموسة للشركات، مثل المعلومات والالتزامات والأوراق المالية أو الملكية الفكرية (براءات الاختراع والعلامات التجارية وقواعد البيانات والبحوث، الخ) التي تدخل في نطاق ذمتها وعلى هذا الأساس يجب أن تكون موضوعا للحماية(2).

1- نحو الاعتراف بحق ملكية البيانات الشخصية.

رغم طبيعتها غير الملموسة فإن الاعتراف بقابلية تملك البيانات الشخصية لا يظهر بوضوح في ضوء الأحكام المنظمة لحق الملكية لكنه أصبح ضروريا

بسبب الممارسات الافتراضية في المجتمع الرقمي (أ). ولكن لا يزال من غير الواضح تماما ما إذا كان بالامكان منح حق الملكية للفرد محل البيانات ومدى حرية تصرفه فيها (ب).

أ- الاعتراف التدريجي بإمكانية تملك البيانات الشخصية.

تعتبر البيانات الشخصية العملة الرئيسية في الاقتصاد الرقمي وموضوع أي مقايضة في هذا المجال. أدى انتشار تكنولوجيات الاعلام والاتصال إلى تخفيض تكاليف جمع وتخزين ومعالجة البيانات. يأخذ جمع البيانات أشكالا متعددة، بدءا من بيانات تصفح مواقع الانترنت إلى تحديد الموقع الجغرافي عن طريق الهاتف المحمول. تسمح رقمنة هذه المعلومات من إنشاء قواعد بيانات ومعالجتها آليا لأغراض مختلفة: الحفاظ على النظام العام، تشخيص الخدمات التجارية أو غير التجارية، تنميط المستهلكين أو المتقدمين للتوظيف، الرقابة على الأنشطة السياسية والنقابية للأفراد، رصد المهاجرين والمسافرين، خدمات التنقل، والتنقيب التجاري، البريد المزعج والاحتيال والنصب عن طريق الإنترنت وغيرها من الاستخدامات سواء كانت مضرة أو مفيدة[1].

تشكل البيانات الشخصية عامل إنتاج مختلف ينشأ في الاقتصاد المتصل بالتكنولوجيات الجديدة. فهي مصدر للسلطة والثروة[2] ولهذا السبب يذهب جانب كبير من الفقه إلى إعتبارها أصولا غير ملموسة. في حين انخفضت القطاعات الصناعية التقليدية بنسبة 3.8٪ بين عامي 2008 و 2011 في أوروبا، فإن

---

[1] Fabrice Rochelandet, « Economie des données personnelles et de la vie privée », La Découverte, Paris, 2010, p. 3.

[2] « the estimated value of EU citizens' data was €315 billion in 2011. It has the potential to grow to nearly €1 trillion annually in 2020 », Viviane Reding Vice-President Reding's intervention at the Justice Council on the data protection reform and the one-stop shop principle, adresse: http://europa.eu/rapid/press-release_SPEECH-13-788_fr.htm

القطاعات التي تعتمد على استغلال البيانات، والتي تشكل الهوية الرقمية أساس عملها (data-intensive sectors) شهدت نموا سنويا يصل إلى 15٪ بالنسبة للتجارة الإلكترونية وحتى 100٪ بالنسبة للجيل الثاني من خدمات الإنترنت- الويب **2.0** - (الشبكات الاجتماعية، الويكي، التطبيقات المتنقلة، الخ)[1]. وقد قدمت الدراسات في هذا المجال الأرقام الأولى عن هذه الظاهرة من خلال أنه

على سبيل المثال ونظرا إلى إيرادات الفيسبوك التي بلغت 5 مليارات دولار مقابل مليار حساب شخصي بمعدل 5 دولارات عن كل حساب شخصي[2].

وبالتالي ومن اللحظة التي نقبل فيها اعتبار المعلومات بما في ذلك البيانات الشخصية كأصول غير ملموسة فإننا نتجه نحو الاعتراف بوجود حق مانع عليها، تطبيقا لمبدأ ناتج عن تملّك المعلومة[3]. تعتبر الملكية وفقا للتصور الحديث مفهوما أساسيا في القانون يعبر عن علاقة بين الإنسان والمال أو الحق تجعله مختصًا به[4]. وبناء على هذه النظرية يأتي رأي الاستاذ كاتلا (Catala) في مقدمة الآراء التي اعطيت للمعلومة وصفاً ذا قيمة اقتصادية. اذ يعتبر أن المعلومة مستقلة عن دعامتها المادية (أي الشيء الذي يحتويها- البحث مثلاً-)، وبكونها قيمة قابلة للتملك (Un bien Susceptible d'appropriation). ويوضح من اجل هذا

---

[1] « The value of our digital identity », Boston Consulting Group Report, Liberty Global Policy Series, nov. 2012.

[2] Caroline Lancelot Miltgen, « Dévoilement de données personnelles et contreparties attendues en e-commerce: une approche typologique et interculturelle », Systèmes d'information & management 4/2010 (vol. 15) , p. 45-91.

[3] Pierre Leclercq, « Essai sur le statut juridique des informations », in « Les flux transfrontalières de données: vers une économie informationnelle », s. dir. d'A. Madec, Doc. Fr., Paris, 1982, p. 123.

[4] Frédéric Zenati-Castaing, Th. Revet, « Les biens », Paris, PUF, 3e éd., 2008.

الوصف بأن المعلومة تقوم وفقاً لسعر السوق، متى كانت غير محظورة تجارياً، وانها منتج، بصرف النظر عن دعامتها المادية وعمل من قدمها وانها بالاضافة الى ذلك ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل بعلاقة المالك بالشيء الذي يملكه. وهي، بهذا الوصف تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما[1].

ومن هنا فإن الاستاذ كاتلا (Catala) يبني تصوره في اضفاء وصف المنتج على المعلومة على حجتين، الاولى: قيمة المعلومة الاقتصادية. والثانية: علاقة التبني التي تجمع بينها وبين مؤلفها، بمعنى ان المؤلف مالك للمعلومة قبل ان يتنازل عنها للمستفيد بموجب العقد. وهذا ما تجري عليه كذلك أحكام القضاء الفرنسي، وخاصة الحكم الصادر من محكمة النقض الفرنسية المعروف باسم Borquin والتي تتلخص وقائعه في قيام عاملين من عمال مطبعة بوركان قاما داخل المطبعة وبأدواتها بتصوير سبعة وأربعين شريطًا أخرى وقاما بتصويرهم خارج المطبعة وعلى ماكيناتهم الخاصة بهدف إنشاء شركة منافسة جديدة فيما بعد، وقدما للمحاكمة بتهمة السرقة، وصدر الحكم بإدانتهم فأيدت محكمة النقض الفرنسية هذا الحكم لتوافر جريمة السرقة ضدهما، والتي تتمثل في سرقة بعض الشرائط وفي سرقة المحتوى ألمعلوماتي للبعض الأخر، وذلك مدة الوقت اللازم لنسخ هذه المعلومات ، وذلك يعد بلا شك اتجاه صريح من محكمة النقض الفرنسية بصلاحية البرامج والبيانات بالرغم من طبيعتها المعنوية لأن تكون محلا للاختلاس ذو الطبيعة المادية.

حيث أن قيام الجناة بنسخ برامج وقواعد بيانات دون رضاء مالكها فعل يتحقق به ركن الاختلاس في جريمة السرقة، وذلك لأن الاستيلاء عليها يتحقق واضحًا جليًا فيما يرتبه النسخ من وقوع البيانات حقيقة وبكل فوائدها ومزاياها

---

[1] Pierre Catala, Les transformatique de driot par L'informatique in Emergence du droit de L'infirmatique des pargues, Paris, 1983, p.168.

الاقتصادية وغيرها تحت سيطرة المتهمين فيصبح بمقدورهم التصرف فيها بحرية وتوجيهها، وبها يظهر المتهمون بمظهر المالك ويغتصبون سلطة مالكها في ذلك بتجريد البيانات من الذمة المالية للشركة.

وتأييداً لذلك حكمت محكمة النقض الفرنسية أيضًا في حكمها الصادر في قضية Logolixa سنة 1979 و التي قررت فيه بأن " إعادة إنتاج مستندات بدون علم ورضاء مالكها يشكل جريمة سرقة، لأن مرتكب هذا الفعل وكان مستخدمًا بأحد المشروعات نسخ عن طريق تصوير مستندات سرية تحتوى على خطة هيكلة المشروع يكون قد استولى بطريق الغش على هذه البيانات ".

ولما كانت قواعد البيانات المعالجة اليكترونيا تعد مالاً بطبيعة الحال باعتبار أن لها قيمة اقتصادية تستحق الحماية القانونية، بالرغم من كونها غير محسوسة، ولكن يمكن ترجمتها في كيان مادي حين تراها شيئًا ماديًا ملموسًا حين تترجم على شاشات الحاسب الآلي في صورة أفكار، وحين تظهر في صورة أوراق مطبوعة، وبالتالي فإن تلك البيانات والمعلومات والتي تنتقل عبر الأسلاك عن طريق انتقال نبضات ورموز تمثل شفرات تتحول إلى معلومات معينة لها أصل يمكن سرقته والاستيلاء عليه وبالتالي فإن لها كيان مادي[1].

وباعتبارها شيئا يمكن للمعلومة أن تكون موضوعا لعقد – بما في ذلك عقد البيع – وبالتالي تتحول إلى سلعة. و كجزء مكون للهوية الرقمية والتراث غير

---

[1] M-P. LUCAS de LEYSSAC, « Une information seule est-elle susceptible de vol ou d’une autre atteinte juridique aux biens ? », D. 1985, chron. p 43 et s. « L’arrêt Bourquin, une double révolution: un vol d’information seule, une soustraction permettant d’appréhender des reproductions qui ne constitueraient pas des contrefaçons », Rev. sc. crim. 1990, p. 487.

المادي للأشخاص الطبيعية والاعتبارية، اكتسبت البيانات الشخصية بالتالي قيمة سوقية: يتم شراؤها وبيعها في شكل دعاية سلوكية وتجارة الملفات. وهي تشكل مصدرا هائلا للفرص الاقتصادية، وتقدّم للشركات التي تقوم بجمعها واستخدامها وحفظها وكذلك لشركائها، امكانيات موسّعة لتطوير الأعمال، وبالتالي الحصول على زبائن جدد. أصبحت هذه البيانات أساس النمط الرئيسي في تمويل خدمات الإنترنت التي يعتمد نموذجها الاقتصادي إلى حد كبير على المجانية (الفيسبوك، وجوجل، الخ). وهكذا ومن خلال الموافقة على استخدام خدمات مثل الشبكات الاجتماعية المجانية، يوافق الأفراد ضمنيا على المتاجرة بالبيانات الخاصة بهم.

ب- حق ملكية البيانات و مجال الامتيازات المرتبطة بها.

إن المتاجرة بالبيانات ظاهرة مزدوجة: في حين أنه مما لاشك فيه تساهم في تطوير التجارة الإلكترونية من خلال تحفيز التدفق الحر للبيانات *(free flow of information)*، ولكن أيضا يمكن لها أن تعرقل تطور التجارة الإلكترونية بسبب عدم الثقة التي قد يشعر بها مستخدمي الانترنت.

في هذا السياق فإن فكرة التحكم في البيانات الشخصية بالحد من حق الملكية بدأت في جذب المفكرين والفقهاء من جميع الاتجاهات الأكاديمية والايديولوجية. ونتيجة لذلك فإن القبول بالمتاجرة بالبيانات الشخصية هي بالفعل حقيقة واقعة في الولايات المتحدة، و تمارس من خلال وسطاء يوصفون بـــ "سماسرة" البيانات *(data brokers)* يعرضون على الأفراد لاستعادة السيطرة على بياناتهم حملهم نحو سوق موجه للمعلنين. وبالتالي يفترض أن البيانات الشخصية قابلة للتقييم والنقل والتسويق، مع التزام وحيد وهو الحصول على مقابل. على هذا النحو فإن الشروط العامة لمثل هذه الخدمات الأمريكية المتعلقة بالسمسرة في مجال البيانات

مثل Datacoup حيث تنص صراحة على أن بيانات المستخدمين التي تخضع لها والتي تباع لها في الواقع، وهذا ما يسمح لها فيما بعد بإعادة بيعها. لذلك وبسعر ثمانية (8) دولارات في الشهر يحصلون على الوصول الحر إلى الملفات الشخصية (خاصة على الفيسبوك وتويتر)، وكذلك على سجل مشتريات المستخدمين على الانترنت الذين يرغبون في ابرام الصفقة. لا يتماشى هذا النهج الآن مع ما هو معمول به أوروبيا والذي يعتمد بدلا من ذلك على تصور "شخصاني"، معتبرا البيانات الشخصية امتدادا للشخصية الانسانية و على هذا الأساس تستوجب الحماية.

في التصور الأوروبي فإن الحق الذي يحوزه مالك البيانات ليس حق الملكية – في مفهوم الفقه الأمريكي – وإنما هو حق الرقابة على معالجة هذه البيانات. وتُبرّر هذه المقاربة بحكم طبيعة البيانات ولا سيما في الواقع الرقمي، حيث تستنسخ البيانات بسهولة وبسرعة، وهو ما يجعل من الصعب الاعتراف بحق حقيقي و ذلك أن مفهوم " الملكية " يتطلب بُعدًا حصريا في العلاقة مع الحيازة. وبالتالي فإن البيانات الشخصية في أوروبا غير قابلة للتصرف ونظريا غير قابلة للتسويق، وفقا لمبدأ عدم الاستغلال التجاري للجسم البشري. يتمثل حق الملكية إذن في الحق في الرقابة على الاستغلال والذي يعتبر حقا شخصيا يمارس من طرف الغير[1]. تم انتقاد القيود المفروضة على المتاجرة بالبيانات الشخصية من قبل الذين يدعمون التطور الحر " للمجتمع المتصل شبكيا ". إن عدم قابلية المعلومات الشخصية للتصرف لا تكون فقط في مواجهة المصالح التجارية للشركات أوروبية التي تواجه منافسة أمريكية شرسة، ولكن و بصفة خاصة في

---

[1] Thomas Saint-Aubin, « Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data). Les droits de l'opérateur de données sur son patrimoine numérique informationnel. », RLDI, n°102, mars 2014, p. 94-101.

مواجهة ممارسات الأفراد أنفسهم الذين لا يجدون اليوم أية مشكلة في نشر بياناتهم الشخصية وفقا لاهتماماتهم ومصالحهم الخاصة. لتلبية احتياجات هؤلاء ظهرت خدمات أوروبية مثل YesProfile التي تقدم حاليا حدا أدنى من الخدمة بالمقارنة مع الحلول الأمريكية لأنها لا تعرض سوى "إيجار" بيانات المستخدم، من أجل ارسالها بموافقته إلى معلنين محددين، حتى يكون بامكانهم ارسال عروض تجارية مباشرة إلى عنوان بريده الإلكتروني. في المقابل يتلقى المستخدم مبلغا ماليا أو يمكن أن يختار منح مداخيله لجمعية خيرية. على هذا النحو يبقى مسيطرا بعض الشيئ على البيانات الخاصة به (ويسمى أيضا التمكين الرقمي « Digital *empowerment* » في الولايات المتحدة) لأنه مالكها الحصري وبالتالي يحتفظ لنفسه بالحق و في أي وقت في المطالبة بوقف جمع ومعالجة البيانات لأغراض تجارية. هذا الاعتراف بالحقوق الاقتصادية للفرد يسمح للمستخدم مالك البيانات الحصول ليس فقط على تعويضات عند انتهاك حقوقه، ولكن أيضا على أوامر جبرية لتفادي الضرر أن يتكرر[1].

في إنتظار تطورات إجتماعية حقيقية فإن الأفراد الذين لا يهتمون بمآل ببياناتهم وأولئك الذين يفضلون بيعها ما زال يفوق عدد أولئك الذين يولون إهتماما حقيقيا لحماية معلوماتهم الشخصية.

2- الحق في حماية البيانات التجارية.

هناك قواعد في تطور دائم تهدف إلى حماية بيانات الشركات على سبيل المثال تلك المتعلقة ببراءات الاختراع والأسرار التجارية أو بمنتجي قواعد البيانات (أ). وإن صعوبة الاعتراف بحق ملكية البيانات تفرض أن يكون في علاقة توازن مع حقوق وحريات أخرى (ب).

---

[1] Pam Samuelson, « Book review. A new kind of Privacy? Regulating uses of personal data in the global information economy », California Law Review, 1999, vol. 87, p. 751.

أ- المعلومة باعتبارها جزءا لا يتجزأ من الأصول غير المادية للشركات والتي في حاجة إلى حماية فعلية.

تساهم الأصول الصناعية وغير المادية في تحقيق الأمن الاقتصادي لكل شركة. ويقصد بالأصول غير المادية "كل ما هو غير مادي وغير قابل للقياس الكمي في حسابات الشركة، ولكنه يشارك في ثروتها المادية. الاعتراف بهذا المفهوم يسمح الأخذ بعين الاعتبار عناصر غير ملموسة وبدون واقع مادي ومالي فوري في الثروة الإجمالية للشركة "[1]. ويشمل خاصة الأصول التكنولوجية و أصول أنظمة المعلومات و الأصول المعلوماتية. تشكل المعلومة إذن عنصرا رئيسيا فيه، تتعلق حمايتها بإشكالية مركزية لأي نشاط إقتصادي في القرن الحادي والعشرين: تتمثل في أمن أنظمة المعلومات. وهكذا فإن جميع بيانات الشركة من المحتمل أن تشكل لها قيمة اقتصادية معينة. وبناء على ذلك ووفقا لقيمتها الاقتصادية الهامة، فإن حيازة المعلومة يفرض بناء وتصميم سياسة أمنية شاملة لنظام المعلومات داخل الشركة ؛ ويجب أن تكون بالضرورة قابلة للتطوير نظرا لطبيعة نظام المعلومات، وأن تتكيف مع النصوص التنظيمية.

و بصفة عامة فإن الهدف من حماية أصول المعلومات للشركة هو الحفاظ على بياناتها في سياق أنشطة الذكاء الاقتصادي في مراحلها الثلاث: جمع و حماية وأمن المعلومات، وأيضا حمايتها من ممارسات التأثير و التأثير المضاد (أو مايسمى بالتضليل). وترتبط حقوق الشركة على بياناتها بالقدرة على استخدام جميع الوسائل لتثمينها: أي تفعيلها أولا، ثم إثراءها وتوزيعها في الأخير. وهكذا يمكن حماية بيانات الشركات من خلال طرق عدة. فيما يتعلق أولا بالبيانات المصنفة سرية يمكن حمايتها بإبرام عقود السرية بين الشركة وموظفيها، الشركاء

---

[1] Christian Bourret et al., « Capital immatériel et information professionnelle. L’émergence d’un concept nouveau:l’information durable », Documentaliste-Sciences de l’Information, 2008/4 vol. 45, p. 4-12.

والمقاولين من الباطن. وهنا يتعلق الأمر بالمعلومات التي أبلغ بها، ولكن يطلب من متلقيها أن لا يكشف عنها أو أن يستعملها بشكل مقيد. ثم لدينا الابتكارات وهي البيانات ذات التطبيق الصناعي، والتي توفر حلا تقنيا لمشكلة تقنية، والتي من المحتمل أن تكون محمية بموجب براءات الاختراع. تطرق المشرع الجزائري إلى البيانات وأطلق عليها مصطلح "المعطيات" في المادة 394 مكرر من قانون العقوبات والتي جاءت في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات التي أضيفت بموجب القانون رقم 04-15 المؤرخ في10 نوفمبر2004 المعدل لقانون العقوبات[1]، والتي تطبق في حالة الدخول عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات. وبالتالي فإن هذه القواعد تحمي البيانات الموجودة في أنظمة المعلومات الخاصة بالشركات.

ب- إمتداد حقوق الشركات على البيانات في مواجهة الحريات العامة.

إن حماية المعلومات من طرف الشركات أصبحت أكثر تعقيدا في مجتمعات تتوق للاتصال وحرية الاعلام، ولأننا في وقت الشفافية والأولوية ليست في المحافظة على السر التجاري[2]. لذلك فمن الضروري أن تهدف القواعد المعمول بها لحماية الحريات الأساسية للفاعلين الاقتصاديين لتحقيق التوازن بين مقتضيين متناقضين أحيانا: الحق في السرّية والحق في المعرفة. هذه الموازنة تؤدي بالتالي إلى اجراء تحكيمات بين قيم مثل الحق في الملكية والحق في حماية البيانات من جهة، وحرية التعبير والحق في الوصول إلى المعلومات باسم مقتضيات عامة من جهة أخرى. في هذا السياق يجب أن يكون الحق في حماية السرّية ليس فقط

---

[1] المقتبس من القانون الفرنسي رقم 88-19 من 5 يناير 1988 المتعلق بالتزوير الالكتروني من اقتراح النائب Jacques Godfrain الذي عرف هذا التشريع بإسمه.

[2] Patrice Spinosi, « Le secret d’affaires et le secret du patrimoine. Face aux droits et libertés individuels », DP, n° 233, févr. 2014, p. 26 à 30.

دفاعا عن أملاك الشركة، ولكن أيضا عن أملاك جميع الأشخاص المساهمين فيها. وخاصة العمال فمن الواضح أيضا أنه من المصلحة المشروعة للشركات أن يتم حماية حياتهم الخاصة وبياناتهم الشخصية.

يكون التوفيق بين حماية بيانات الشركة والحفاظ على حقوق أخرى أمام إختبار صعب لا سيما في حالة اجراءات التفتيش والحجز التي تأمر بها المحاكم في إطار التحقيق، إما عن طريق حجز المعدات أو الأملاك عن بعد. على هذا النحو ومن بين الحقوق والحريات الأساسية التي تأتي لدعم وحماية الملكية الفكرية للشركات، نجد في مقدمتها الحق في حرمة الحياة الخاصة من منظور الحق في حرمة المسكن[1]. أكدت محكمة حقوق الإنسان الأوروبية في عدة مناسبات على ضرورة احترام الضمانات الإجرائية خلال اجراءات التفتيش والحجز لحماية الأسرار التجارية[2].

ومع ذلك يمكن لحريات أساسية أخرى أن تتعارض مع احترام الأسرار التجارية، مما يجعل من الضرورة تحقيق التوازن بين الحقوق المختلفة. ويتعلق الأمر بصفة خاصة بمقتضى الشفافية الذي يظهر من خلال حق اعلام الجمهور النابع من حرية التعبير المكفولة للمواطنين. يتميز حق الاعلام بطابع مزدوج، من جهة بأن له أثر إيجابي في الوسط الصحفي بضمان حرية التعبير للصحفيين، ومن جهة أخرى أنه يتحول بشكل متزايد إلى نموذج فردي لكل مواطن يمكن استخدامه ضد الأسرار دفاعا عن المصلحة العامة[3] ككشف الأسرار التجارية حماية للمستهلك مثلا.

---

[1] CEDH, 1ère sect., 14 mars 2013, aff. 24117/08, Bernh Larsen Holding As. Et a. c/ Norvege.

[2] CEDH, 3ème sect., 21 févr. 2008, aff. 18497/03, Ravon et a. c/ France, § 26 ; CEDH, 5e sect., 21 déc. 2010, aff. 29408/08, société Canal Plus et a. c/ France, §37.

[3] وبهذه المناسبة وفي سياق القضايا البارزة مثل قضية "ويكيليكس" أو "سنودن"، أصبحت قضية "المبلغين عن الفساد" وفرضت نفسها بشكل واضح في تفكير القضاة. ولكن في عام 2004، دعا

أصبحت شبكة الإنترنت في وقت قصير مسرحا رئيسيا للجرائم التقليدية مثل الجريمة المنظمة والإرهاب والاعتداء الجنسي على الأطفال، الخ. ولكن تشكل أيضا مجالا خصبا لأنواع جديدة من الجرائم، مثل انتحال الهوية الرقمية أو التحميل غير المشروع.

المقرر الخاص للأمم المتحدة المعني بحرية التعبير، ونظيره في منظمة الدول الأمريكية، وممثل منظمة الأمن والتعاون في أوروبا(OCSE) ، الحكومات بشكل مشترك إلى حماية المبلغين عن الفساد من "أي عقوبات قانونية أو إدارية أو مهنية إذا تصرفوا بحسن نية".

المراقبة الرقمية: الضبط الاداري في مواجهة منطق الإنترنت.

سوف نرى إلى أي مدى قد تعرض إساءة استخدام وسائل الاتصال الإلكترونية سلامة الأشخاص والممتلكات وكذا النظام العام للخطر. وأصبح هناك اليوم حاجة ملحة لإيجاد توازن بين من جهة الحريات العامة مثل حرية التعبير والحقوق المنافسة والتزام الدولة في المحافظة على النظام العام من جهة أخرى و ذلك من خلال المراقبة الرقمية. والتي تمس بالحريات العامة من خلال تشريعات تبررها المقتضيات الأمنية. وهكذا وكلما تم تبني قواعد بهدف ضمان أمن الأفراد والحفاظ على النظام العام، وحماية مستخدمي الإنترنت من الاجرام الرقمي، تقوم السلطات بذلك في المقابل بتقييد حريات المواطنين الأساسية.

المخاطر المرتبطة بإساءة استخدام الانترنت.

سنتطرق أولا إلى جرائم الإنترنت الموجهة مباشرة ضد البيانات في أنظمة المعالجة الآلية للبيانات (فرع أول). ثم إلى تلك التي تتم من خلال المحتوى المنشور على الانترنت و التي تمس بحقوق الأشخاص (فرع ثاني). وتتكون الفئة الأخيرة من أنواع متعددة من الجرائم الإلكترونية تشكل مخاطر معينة على حياة وأمن الأشخاص وعلى النظام العام (فرع ثالث).

التعدي على البيانات الرقمية.

يمكن أن يأخذ تعريض البيانات الرقمية للخطر شكل هجوم يهدف إلى انتهاك سلامتها وسريتها وأمنها أو توفرها (أولا). و هناك جرائم أخرى خاصة بالبيانات

تتعلق بالاعتراض غير القانوني لها (ثانيا)، وأخيرا ما يتعلق بالتزوير الالكتروني (ثالثا).

أولا: المساس بسلامة وأمن البيانات.

يمكن أن يكون المساس بسلامة وأمن البيانات بشكل غير مباشر أي ناتجا عن اختراق الأنظمة المعالجة لها (1)، ومن جهة أخرى بشكل مباشر مثل الدخول عن طريق الغش أو الحذف(2).

1- الخطر المحتمل على البيانات نتيجة الوصول غير المشروع إلى أنظمة المعالجة الآلية.

مع تطور الشبكات الالكترونية أصبحت جريمة الدخول غير المشروع إلى أنظمة المعالجة الآلية للبيانات ظاهرة منتشرة[1]. حيث أصبح من الصعب على نحو متزايد الحفاظ على سرية البيانات الواردة في الأنظمة.

يكون الاعتداء على أنظمة المعالجة الآلية للبيانات من الناحية التقنية وفي معظم الحالات من خارج الأنظمة، ويستهدف البيانات ويحتاج في معظم الحالات الدخول إلى أنظمة تخزين هذه البيانات. وبالتالي فإن قمع جريمة الدخول غير المشروع إلى أنظمة المعالجة الآلية للبيانات يشكل خطوة أولى نحو ردع جرائم مثل تعديل أو اعتراض البيانات.

وهكذا يميّز القانون رقم 04-15 المؤرخ في10 نوفمبر2004 المعدل لقانون العقوبات بين صورتين: الصورة البسيطة للجريمة وتتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة تتحقق بالحالة التي ينتج فيها عن

---

[1] Jeffrey Kephart, Steve White, David Chess, « Computer viruses: a global perspective », 5th Virus Bulletin International Conference, Boston, 20-22 sept. 1995, Virus Bulletin Ltd, Abingdon, England, p. 165-181.

الدخول أو البقاء غير المشروع إما حذف أو تغيير معطيات المنظومة أو تخريب لنظام اشتغالها.

تعاقب المادة 394 مكرر قانون العقوبات: " كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة.

في الأخير نصت المادة 394مكرر 3على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام أي إذا استهدفت البيانات المعالجة من طرف الدولة.

تجدر الاشارة أنه في النظام الجزائري يتحقق الركن المادي للجريمة بالبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات بغض النظر عن نتيجة سلوك مرتكبها، فهذا الأخير معرّض للعقوبات حتى في غياب ضرر. في حين أن بعض التشريعات لا تفرق بين جرائم الدخول والبقاء في أنظمة المعالجة الآلية للبيانات[1]، وأخرى تعاقب فقط على الدخول بطريق الغش في حالة انتهاك خطير (على سبيل المثال في حالات التحايل على التدابير الأمنية[2]، أين يقصد الفاعل الفعل الضّار)،

---

[1] Joel R. Reidenberg, « States and Internet Enforcement », University of Ottawa Law & Technology Journal, vol. 1, n°213, 2004, p. 213, adresse: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965.

[2] كما هو الحال في النظام الألماني على سبيل المثال، حيث تجرم المادة 202 a1 من قانون العقوبات االتجسس الالكتروني وتنص على أنه "من يحصل بدون ترخيص على إمكانية الوصول، له أو لشخص آخر، إلى بيانات غير مرسلة إليه ولها حماية خاصة من الوصول غير المصرح به، بالتحايل على هذه الحماية، يعاقب بالحبس لمدة تصل إلى ثلاث سنوات أو بغرامة ". وكذلك يقضي القانون البرازيلي رقم 12.737 / 2012 بضرورة وجود حماية لقاعدة البيانات بحيث يمكن تحديد جريمة الوصول غير القانوني. وأخيرا تطبيقا للمادة 615 من قانون

أو عند الحاق حد أدنى من الضرر، أو عند المساس بأنظمة المعالجة الآلية للبيانات ذات أهمية خاصة أو المساس بالبيانات الموجودة في هذه الأنظمة[1]. إن غياب التنسيق بين الدول في هذا المجال راجع إلى مضمون اتفاقية مكافحة الجرائم الإلكترونية التي تترك للدول الموقعة حرية وصف جرائم الدخول والبقاء في أنظمة المعالجة الآلية للبيانات، فعلى سبيل المثال تنص المادة 42 من الاتفاقية على أنه لا يمكن للدول الموقعة تجريم فعل الوصول إلى أنظمة المعالجة الآلية للبيانات إلا إذا كانت هذه الأنظمة مربوطة بشبكة الانترنت، حيث لا تجرم الحالات التي يصل فيها القراصنة إلى هذه الأنظمة، دون الحاجة إلى شن هجوم عبر الإنترنت. تجدر الاشارة أن الجزائر لم تصادق على اتفاقية بودابست وهي أول معاهدة دولية تسعى إلى معالجة الإنترنت وجرائم الحاسوب عن طريق موائمة القوانين الوطنية لكل دولة، وتحسين أساليب التحري وزيادة التعاون بين الدول، و اكتفت بالمصادقة في 2014 على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات و التي جاءت مطابقة لأحكام اتفاقية بودابست خاصة على مستوى القواعد الاجرائية، سواء من حيث نطاق التطبيق أو طبيعة هذه القواعد، حيث

العقوبات الإيطالي، لا يوجد وصول احتيالي إلا إذا كان النظام محمي بتدابير أمنية. ومن ناحية أخرى، فإن العيب التقني الذي يؤدي إلى تيسير التحايل على التدابير المتخذة لا يعتبر عيبا في التدابير الأمنية. لتحليل التشريعات الأمريكية المطبقة في هذا السياق أنظر:

H.M. Jarrett, M.W. Bailie, « Prosecuting computer crimes », Office of Legal Education Executive Office for United States Attorneys, adresse: http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

[1] وفي هذا الصدد ينص القانون البرازيلي رقم 2012/1237 على نظام تدرجي في قمع الجرائم الالكترونية يميز وفقا لخطورة عواقبها أو طبيعة ضحاياها. وبالتالي فإن تقييم الوقائع لن يكون هو نفسه حسب ما إذا كان الوصول إلى البيانات يؤدي إلى خسائر اقتصادية، أو تعلق بمعلومات سرّية، مثل الاتصالات الخاصة أو الأسرار التجارية أو الصناعية أو المعلومات المصنفة على أنها سرية بموجب القانون. أو تتحقق بواسطة جهاز تحكم عن بعد، أو أن يكشف الفاعل عن المعلومات التي وصل إليها أو يتاجر بها، أو أن فعله قد ارتكب ضد موظفي الدولة.

نصت على مجموعة من القواعد الاجرائية أوجبت على الدول الأطراف ملاءمتها مع قوانينها الوطنية فيما يتعلق لاجراءات الجزائية كتدابير التحفظ على بيانات الكمبيوتر المخزنة و كشفها و اصدار الأوامر بتسليمها و اجراءات التفتيش على البيانات المخزنة وحجزها و التجميع الفوري لها و اعتراض محتواها و ذلك من خلال المواد من 23 إل 29 من الاتفاقية[1]. وعلاوة على ذلك، بعض القضاة، كالقاضي الألماني الذي تطرق إلى مسألة تدرج الإجراءات الأمنية و في أي مرحلة يؤدي خرقها إلى قيام الجريمة. حيث لا تقوم الجريمة في ألمانيا إذا كان الإجراء الأمني سهل الاختراق وبدون عناء، أو كان غير فعّالا بالنسبة للمحترفين.

2- مختلف الجرائم المتعلقة بالبيانات.

تنص المادة 394-1 من قانون العقوبات الجزائري على أنه " يعاقب بالحبس من 06 أشهر الى 03 سنوات و بغرامة من 500.000 دج الى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها". يردع هذا النص أي تغيير أو حذف أو تعديل للبيانات الموجودة في أنظمة المعالجة الآلية للبيانات و ذلك مهما كانت نتائج ذلك الفعل. إن فعل الادخال يجب أن يكون عمدا وبطريق الغش أي بتوافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش و إرادة تسبيب ضرر للغير. إن الأفعال المجرمة على هذا الأساس تتعلق إذن بأي مساس بالبيانات والملفات أو قواعد بيانات. إن هذا المساس قد يأخذ شكل إدخال بيانات جديدة أو حذف بيانات موجودة. من ناحية أخرى ليست مجرّمة بموجب

---

[1] هشام ملاطي، خصوصية القواعد الإجرائية للجرائم المعلوماتية-محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية-، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع،2014، ص83.

المادة 394-1 أفعال النسخ والارسال أو ربط البيانات مادامت هذه البيانات لم تتعرض لأي تغيير[1]. النص هو حماية في الواقع للبيانات كجزء من أنظمة المعالجة الآلية للبيانات التي لا ينبغي أن يتم ادخال تعديلات عليها بدون رخصة وليس حماية لمحتواها، أو للمعلومات التي تتضمنها أو لقيمتها[2].

وهكذا فإن إدخال البيانات بطريق الغش في أنظمة المعالجة الآلية للبيانات هي من الجرائم الأكثر إنتشارا.

وفيما يتعلق بحذف البيانات والذي يشكل ظرفا مشددا لجريمة الدخول إلى أنظمة المعالجة الآلية للبيانات يمكن أن يؤدي إلى عرقلة عملها (المادة 394 ف2)، وفي هذه الحالة تقوم الجرائم الثلاث[3]. على وجه التحديد فإن التخريب الناجم عن الفيروسات يشكل الفرضية الأكثر انتشارا لحذف البيانات الرقمية. كان في الماضي يتم ادخالها في أنظمة المعالجة الآلية للبيانات باستخدام وسيط مادي (مثل القرص المرن)، بدلا من ذلك ينتشر الفيروس اليوم من خلال الشبكة (مثل رسائل البريد الإلكتروني أو الملفات المحمّلة الملوثة). في هذا السياق، في حين أن بعض البرمجيات الخبيثة تقوم تلقائيا بحذف البيانات، والبعض الآخر يعمل على أساس التشفير وتقوم على سبيل المثال بجعلها غير متاحة للمستخدمين بدون مفتاح فك التشفير دون حذفها بشكل نهائي. بالفعل فحسب التعليمات التي وضعها مصمموه في البداية يقوم الفيروس بسحق أو نشر أو محو أو نسخ أو اضافة أو تغيير البيانات المستهدفة. حول هذه النقطة اعتبرت محكمة الاستئناف بباريس أن

---

[1] Émilie Bailly, « L'entreprise face aux risques informatiques: les réponses du droit pénal », RLDA 2011, n° 64.

[2] Hervé Croze, « L'apport du droit pénal à la théorie générale du droit de l'informatique», JCP 1988. I. 3333.

[3] CA Paris, 8 juin 2012, Dr. pénal n° 12, 2012. chron. 10, obs. Lepage.

إدخال فيروس في نظام الاعلام الآلي يُعبّر بشكل قاطع عن ارادة الجاني المتعمدة والتي تميّز الركن المعنوي للجريمة[1].

وأخيرا وفي سياق السمعة الرقمية: ترتبط حوادث إختراق البيانات برهانات رئيسية، ويتضح ذلك من خلال قضايا حديثة متعلقة بالكشف عن صور خاصة مخزّنة في السحابة الالكترونية والتي أدى نشرها إلى المساس بخصوصية الأشخاص.

ثانيا: الاعتراض غير القانوني.

من اللحظة التي نرسل فيها بيانات عبر الشبكة، تكون هناك مخاطر تتمثل في امكانية اعتراضها. يتمثل اعتراض البيانات في التقاط المراسلات الإلكترونية (رسائل البريد الإلكتروني المرسلة والمستلمة، منشورات منتديات المناقشة، إلخ) والبيانات الرقمية التي تمر عبر الشبكة (عند تحميل الملفات أو التوصّل إلى وسائط تخزين خارجية مثلا). وعلى الرغم من أدوات التشفير المختلفة المستخدمة بشكل متزايد، فمن الممكن فك تشفير البيانات المتبادلة بين الخوادم أو بين الخادم والمحطة. هذا ما حدث على سبيل المثال في عام 2007 في ايطاليا عندما أتهم 20 موظفا من شركة اتصالات ايطاليا بجمع وفك تشفير محتوى إتصالات العديد من الشخصيات كالسياسيين والرياضيين و رجال الأعمال و أستخدم للحصول على مكاسب مالية عن طريق الابتزاز.

ومع ذلك فإن التقنيات المستخدمة لاعتراض البيانات، مثل تقنية المراقبة المعمّقة للحزمات[2] يمكن لها أيضا أن تخدم هدفا نزيها – مثل ضمان عدم وجود فيروس داخل حزمة البيانات المنقولة – كما يمكن لها أن تخدم هدفا سيئا: المتمثل في سرقة المعلومات أو مراقبتها. وهذا هو أيضا هدف مجرمي الانترنت الذين

---

[1] CA Paris, 14 janv. 1997, JurisData n° 020128.

[2] DPI (Deep Packet Inspection).

يمارسون شكلا من أشكال الاستحواذ غير العادل على المعلومات والنصب، المستخدمة في الاعلام الآلي للحصول من الغير على سلعة أو خدمة أو معلومات قيّمة. يجب اعتبار هذه التقنية على أنها شكل من أشكال إعتراض البيانات، على الرغم من أنها تتطلب تثبيت برامج تعمل على اكتشاف منافذ غير محمية أو تجنب التدابير الأمنية، لكن يبقى طابعها بشري أكثر منه تقني. حيث تشكل نشاط تضليلي يكون هدفه حمل الغير بخداعهم على خرق الإجراءات الأمنية العادية. وهناك أدوات مختلفة لتنفيذ هذا النوع من الهجمات، مثل "برامج التجسس" (spyware)، من بينها مسجلي ضربات لوحة المفاتيح (Keylogger).

لذا بادرت العديد من الدول بحماية استخدام خدمات الاتصالات من خلال تجريم أنشطة اعتراض – الاتصالات الهاتفية ثم الالكترونية عموما – والتي يجب اعتبارها من حيث المبدأ غير شرعية، إلا إذا كانت بإذن قانوني. وبهذه الطريقة فإن منع اعتراض المراسلات الإلكترونية يرتبط إلى حد كبير بخصوصيتها وبسرية المراسلات.

وغالبا ما يتم تبني قواعد تتوافق مع تلك المقترحة في المادة 3 من الاتفاقية المتعلقة بجرائم الإنترنت التي تجرم الاعتراض غير القانوني لعمليات نقل البيانات. والتي تهدف إلى تكيّيف حماية المراسلات الالكترونية مع حماية الاتصالات ضد التنصت غير الشرعي والتسجيلات الموجودة سابقا في معظم النظم القانونية. ووفقا للتقرير التوضيحي يعتبر اعتراضا غير قانوني "التنصت وتسجيل البيانات." وكما هو الحال بالنسبة للدخول غير المشروع: تترك الاتفاقية للدول الموقعة عليها حرية تحديد معايير قيام جريمة الاعتراض غير القانوني وذلك سواء بانتهاك بعض التدابير الأمنية أو بتوفر قصد جنائي.

يستشف من هذه القواعد القانونية أنها تهدف إلى المحافظة على البيانات – لاعتبارها معلومات شخصية خاصة بلأفراد أو أصول غير ملموسة خاصة

بالشركات – ضد أشكال مختلفة من التجسس. وهكذا فإن جريمة الاعتراض غير القانوني تدخل في إطار التشريعات الرادعة للتجسس على البيانات، و سواء كانت هذه البيانات متعلقة بمجالات محددة[1] أو بيانات حاسوبية بشكل عام[2]. ولكن يبقى أن العديد من الدول تتعرض لمقتضى احترام سرية الاتصالات الالكترونية للمواطنين من خلال الاحتفاظ بامكانية استخدام نفس النوع من تقنيات اعتراض البيانات في إطار المتابعات القضائية. في الجزائر على سبيل المثال يمكن للسلطات القضائية، في جرائم معينة، اعتراض وتسجيل المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية عندما (المادة 65 مكرر5 إلى المادة 65 مكرر10 من قانون الإجراءات الجزائية).

ثالثا: التزوير الالكتروني.

بهدف ردع أعمال التزوير أو الغش الالكتروني جاءت اتفاقية بودابست بمادتين. حيث تجرم أولا في المادة 7 " إدخال وتخريب، أو الحذف المتعمد دون وجه حق للبيانات الالكترونية، مما أدى إلى خلق بيانات زائفة بقصد أن تؤخذ بعين الاعتبار أو أن تستخدم لأغراض قانونية كما لو كانت أصلية، و قد تكون مباشرة أم لا تكون مفهومة و قابلة للقراءة ".

---

[1] في الولايات المتحدة على سبيل المثال يجرم قانون التجسس الاقتصادي لعام 1996 (18 U.S.C. § § 1831 وما يليها) التجسس على البيانات الاقتصادية وغيرها من وسائل الحصول على المعلومات السرية. وعلى الرغم من أن هذا القانون يركز على حماية المحتوى (الأسرار التجارية) ولا يقصد أي شكل محدد (بيانات حاسوبية)، فإنه لا ينطبق فقط على الجرائم التقليدية، وإنما ينطبق أيضا على الجرائم الالكترونية. أنظر:

D.J. Loundy, « Computer Crime, Information Warfare, and Economic Espionage », 2009, p. 55.

[2] إن التجسس على البيانات الاقتصادية وغيرها من البيانات، على سبيل المثال، تعاقب عليه المادة 212 (أ) من القانون الجنائي الألماني المذكورأعلاه.

وبعبارة أخرى فإن الجريمة المقصودة تتمثل في تعديل بيانات من أجل إعطائها قوة إثبات مخالفة للحقيقة وتشكل بذلك وثيقة مزورة يمكن بها تغليط الغير[1].

ثم تشير ثانيا المادة 8 من الاتفاقية إلى تجريم "أي إدخال أو تخريب أو حذف لبيانات معلوماتية و أي مساس بسير نظام معلوماتي يتسبب عمدا في ضرر مادي للغير ويكون بقصد الحصول دون وجه حق على منفعة اقتصادية له أو للغير"[2]. نستنتج أن معيار المنفعة الاقتصادية التي تم الحصول عليها بعد تزوير البيانات هو المعيار الراجح.

بعض الدول مثل بلجيكا تحافظ على نفس التفرقة بين الجريمتين، باعتبار الأولى كتزوير الكتروني والثانية كنصب و احتيال الكتروني.

وفي هذا السياق يمكن تعريف التزوير الالكتروني على أنه تحريف للبيانات الرقمية: وذلك بإنشاء وثيقة تبدو على أنها صادرة عن مؤسسة موثوق بها، وتحريف لصور إلكترونية (على سبيل المثال صور مقدّمة كأدلة أمام المحاكم) وتخريب لوثائق موجودة أصلا. وهكذا يمكن للتزوير أن يكون بعديا، أي أن المجرم الالكتروني يعدّل كتابة موجودة وأصلية بهدف تخريب المحتوى و حذف معلومات منها أو إضافة أخرى جديدة. من ناحية أخرى فإن التزوير من العدم يتمثل في إنشاء دليل كاذب بدون الرجوع إلى كتابة أصلية.

إن دوافع ارتكاب الجريمتين تختلف، حيث أن الذي يقدم وثيقة مزورة بإتلاف وثيقة موجودة أصلا يبحث بشكل عام على تجنب متابعات قضائية محتملة. على هذا النحو وعلى سبيل المثال فمن أجل طمس آثاره بعد قرصنة معلوماتية، يحاول القرصان الالكتروني تغيير معلومات السجل االكتروني الذي يتم فيه الاحتفاظ

---

[1] V. Rapp. explicatif de la Convention, n° 81 et 83.

[2] V. Rapp. explicatif, n° 86.

بأدلة مروره في نظام المعالجة الآلية للبيانات. على العكس من ذلك فإن الذي ينشئ وثيقة مزورة يهدف إلى إنتاج آثار قانونية لصالحه أو لصالح شخص آخر.

لم ينص المشرع الجزائري صراحة على هذه الجرائم ولكن يبدو أنها تقع تحت طائلة المادة 394 مكرر و 394 مكرر 1 من قانون العقوبات التي لا تحتاج إلى القصد الخاص المذكور في الاتفاقية.

وأخيرا وعلى الرغم من أن خطر التزوير قائم، إلا أنه من الممكن حاليا تعزيز الأمن في مجال مصداقية أنواع معينة من الوثائق من خلال إدخال نظام التوقيع الإلكتروني. وهكذا فإن أدوات التشفير في خدمة الأمن من خلال الشهادات الإلكترونية التي تضمن سرية البيانات أو مصداقية التوقيع الإلكتروني[1].

المساس بحقوق الأشخاص.

بعد التطرق للجرائم المتعلقة بنشر مضامين مضرة للأشخاص على الإنترنت (أولا)، سوف نركز على الاعتداءات المختلفة التي يمكن أن تتعرض لها المعلومات الشخصية (ثانيا).

أولا: الجرائم المتعلقة بالمحتوى الرقمي.

الجرائم التي ترتكب عن طريق الصحافة تتعلق بالطابع غير المشروع للمحتويات المنشورة على الانترنت وبالتالي ينص عليها التشريع المتعلق بحرية الصحافة (1). هذه الفئة من الجرائم تتعلق بالمحتويات التي تعتبر غير قانونية، بصفة خاصة المواد الإباحية والعنصرية أو الاساءة إلى الرموز الدينية. بالاضافة إلى ذلك وفي هذه الفئة من الجرائم يكون الأشخاص المعرضين للخطر كالأحداث

---

[1] Éric A. Caprioli, « Signature électronique et dématérialisation », LexisNexis, 2014, p. 175-182.

عرضة بشكل خاص للانتهاكات (2). وأخيرا فإن البريد الالكتروني المزعج يشكل جريمة تتعلق بنشر محتويات مضرّة على نطاق واسع (3).

1- جرائم الصحافة.

إن الإنترنت كوسيلة من وسائل الإعلام العامة الإلكترونية تشكل بيئة مواتية لارتكاب شتى أنواع الجرائم من قذف و سب (أ)، إلى نشر مواد عنصرية تتسبب في ارتكاب الجرائم أو في تفشي ظاهرة الإرهاب أو الاشادة به (ب) إلى إنتشار جريمة الأخبار الكاذبة (ج).

أ- القذف و السب.

ينبغي التمييز بين فعل القذف و السب. في حين عرّف المشرع الجزائري القذف في المادة 296 من قانون العقوبات على أنه " يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة " و السب في المادة 297 على أنه " يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة". يكمن الفرق في أنه لا يشترط في السب اسناد واقعة معينة. من ناحية أخرى فإن القاسم المشترك بين الجريمتين أنهما تهدفان إلى ردع المساس بشرف الأشخاص.

ب- العنصرية و أعمال الاستفزاز والاشادة.

الإنترنت هو بلا شك وسيلة نشر سهلة وشاملة للفكر أو التعبير العنصري، الذي يؤدي إلى ارتكاب الأعمال الإجرامية والعنيفة. يعرف هذا النوع من المحتوى "الذروة" على الشبكة و يرتبط مباشرة بأحداث الساعة و يتزايد تفاعلا مع الأحداث الاجتماعية والسياسية مما يتسبب في سلوكيات متطرفة. إن الاعتداءات والجرائم بدافع العنصرية وكراهية الأجانب والتعصب الديني، أو الهوية الجنسية للشخص أمثلة لجرائم الكراهية التي قد تطال أي مواطن.

يعتبر الحث على إرتكاب هذا النوع من الأعمال في بلدان الكومنلوث شكلا من أشكال المشاركة الجنائية، بينما تعتبره دول القانون الروماني تحريضا. في سياق غياب مفهوم متجانس، يظهر أن هناك خيط رفيع بين حرية التعبير ولغة

التحريض على مثل هذه الأعمال أو التصرفات كالكراهية العنصرية وارتكاب الجرائم المختلفة أو أكثر من ذلك ارتكاب الأعمال الإرهابية.

ج- جنحة المعلومة الكاذبة.

إن الوفرة المعلوماتية التي يغرق فيها المستخدمون اليوم من السمات الرئيسية التي تميّز الاقتصاد الرقمي. و إنّ الانترنت هي بالتأكيد مصدر هائل للمعلومات على الصعيد العالمي. أصبح من السهولة اليوم ممكنا نشر محتويات معلوماتية قد يساء استخدامها من قبل الناشرين. مرونة الاتصالات – واحدة من نقاط القوة الرئيسية لشبكة الإنترنت – قد تتحول إلى انحرافات. من حيث المبدأ فإن محرري المحتوى المعلوماتي – سواء كانوا كتابا أو مصممين أو منتجين أو مخرجين لمواقع الويب أو وكالات الأنباء – ملزمون بتحري الدقة ويجب عليهم إذن تقديم معلومات مشروعة وموثوق بها. إن المخاطر المتصلة بالتجاوزات التي تميّز تقديم المعلومة عن طريق الانترنت تتمثل بصفة خاصة في: التضليل الاعلامي وتخمة المعلومات. إن السيناريو المتشائم لتنمية معالجة المعلومة في الشبكة الرقمية و الذي تطرق إليه بعض الكتّاب، و المتخوفون من أن تحرم الانترنت مستخدميها من فوائد السرية، دون أن تقدم في المقابل شفافية حقيقية[1].

2- المساس بحقوق القصر.

إن القصر فئة اجتماعية تستخدم الإنترنت على نطاق واسع جدا وعلى هذا النحو فإنه من الضروري أن تكون حمايتهم ضد الانحرافات قوية بشكل خاص، بالاستعانة بقواعد غير مؤلوفة في القانون الخاص. بالإضافة إلى المخاطر العامة التي نعيشيها جميعا في مواجهة تكنولوجيا المعلومات والاتصالات (الكشف عن

---

[1] Laurent Cohen-Tangui, « Le clair-obscur d'internet: Transparence et secret », Pouvoirs, n° 97, 2001, p. 85 et s., spéc. p. 89.

البيانات الشخصية، والتشهير، والقذف و المساس بالصورة و التحرش الالكتروني، الخ)، فإن القصّر بصفة خاصة عرضة للخطر عندما يواجهون في لقاءات محتملة أشخاصا خطرين على منتديات النقاش أو الدردشة، وعندما يطلعون على محتويات غير مشروعة (البيدوفيليا، عنصرية) أو مخصصة للكبار (إباحية أو عنيفة). في الحقيقة حتى المحتويات غير المحظورة يمكن أن تشكل خطرا من اللحظة التي من المرجح أن يطلع عليها جمهور شاب. الذي و بسبب هشاشته الخاصة، يمكن للانترنت الفاسدة أن تكون مصدر ضعف، أن تساعد على تنمية مختلف أنواع الادمان، أو على ظهور سلوك مرضي أو منحرف، مثل العنف[1].

3- الدعاية المزعجة.

يتمثل البريد المزعج ("سبام"[2]) في الارسال الكثيف لرسائل غير مرغوب فيها. تم استعمال هذه العبارة في مجال الاعلام الآلي للاشارة إلى "عسر الهضم" لبرنامج أو نظام يسببه هذا الارسال الكثيف للبيانات. انتشرت اليوم ظاهرة البريد المزعج على نطاق واسع جدا، حيث يرجع ذلك إلى أن الأدوات المصممة

---

[1] Bertrand Seys, « Place et rôle des usages des TIC dans la souffrance psychologique », GET Telecom, Actes du colloque « Internet, jeu et socialisation », 5-6 déc. 2002, p. 13.

[2]كلمة "سبام" هو اسم ماركة لقطعة لحم كانت تسوق من طرف شركة هورميل للأغذية Hormel Foods وهي مركبة من SPiced hAM بمعنى لحم خنزير متبل، وأما ربطها بهذا الاسم يعود إلى سكاتش كانت تقوم إحدى الفرق الكوميدية الأمريكية التي تدعى مونتي بيثون , وتعود أحداث المسرحية في مطعم متخصص في بيع قطع لحم الخنزير من نوع السبام وبدخول أحد الزبائن يحاول هذا الزبون المسكين طلب شيء آخر غير السبام تكثر الضوضاء في المطعم ويبدؤون بالغناء بصوت مرتفع "سبام سبام سبام....". حتى انه لم يعد يسمع طلبه. ويدعى ممتهني هذا النوع من الرسائل بالسباميين أو السبامر (spammers) ، وهي كلمة ازدرائية!

للتوزيع الشامل لرسائل البريد المزعج على شبكة الإنترنت متاحة بحرية للمستخدمين من طرف كبار مقدمي خدمات الاعلام الآلي[1]. ومع ذلك فإن هناك أضرار عدة تنجم عن هذه الجريمة. أولا فإن البريد الالكتروني المزعج يمس بالحياة الخاصة للأفراد، باثقال بريدهم الإلكتروني لتشجيعهم على شراء المنتجات غير المشروعة، و بافساد أجهزة الكمبيوتر الخاصة بهم أو أكثر من ذلك بمحاولة سرقة بياناتهم. وهو يمثل شكلا حقيقيا من أشكال التحرش المعلوماتي الماس بتصور معين لحرية المستهلك، وهو وسيلة لانتهاك حياتهم الشخصية أو حتى المهنية.

ثم إن البريد الالكتروني المزعج يشكل أيضا مصدر إزعاج للأشخاص المعنوية التي يتم تزوير العلامة أو الرمز من خلال عمليات التصيد التي تخدع المستهلك مما يتسبب في المساس بهويتها الرقمية. وأخيرا فإن الشركات مثل متعاملي الاتصالات ومزودي خدمات الإنترنت يعانون أيضا من ظاهرة الرسائل غير المشروعة، التي يحتل فيها البريد المزعج جزءا كبيرا من عرض النطاق الترددي على حساب التطبيقات المشروعة، مما يتسبب على سبيل المثال في طوابير انتظار لنقل رسائل المستخدمين. وهذا يولّد تكاليف إضافية لأنهم مجبرون على توسيع بنيتهم التحتية. وأفاد تقرير عن التهديدات الموجودة على الإنترنت الصادر في أفريل 2014، والمتعلق بالثلاثي الأول من سنة 2014، عن ارسال ما يعادل 54 مليار رسالة من البريد الالكتروني المزعج يوميا[2].

---

[1] من الخدمات الرقمية التي تأثرت بشكل خاص بالبريد المزعج هي خدمة تويتر، التي قدمت في عام 2012 بشكوى ضد العديد من موفري أدوات البريد المزعج – مثل TweetAdder, TweetBuddy, Troption , Justinlover – مشيرة إلى: " يواصل مهندسونا محاربة جهود مرسلي الرسائل غير المرغوب فيها في التحايل على وسائل الحماية لدينا واليوم نضيف سلاحا جديدا إلى ترسانتنا: هو القانون."

[2] Cyberoam, « Internet threats trens report », avr. 2014, adresse:

لمكافحة البريد المزعج قام العديد من مقدمي خدمات البريد الإلكتروني بتثبيت أنظمة مكافحة البريد المزعج (مرشحات أو فلاتر) التي تمنع رسائل البريد الإلكتروني الضارة باستخدام كلمات مفتاحية أو قوائم سوداء تحتوي على عناوين بروتوكول الانترنت IP الخاصة بالمخالفين.

ثانيا: الجرائم الماسة بالبيانات الشخصية للأفراد والبيانات السرية للأشخاص المعنوية.

كما سنرى هناك جرائم تتعلق أولا بعدم احترام حقوق الأفراد على بياناتهم الشخصية (1)، وثانيا جرائم تتعلق بالتعدي على الأصول غير الملموسة للأشخاص المعنوية (2).

1- انتهاك حقوق الأفراد على بياناتهم الشخصية.

عموما يمكن أن تنتهك هذه الحقوق من خلال أعمال سواء في إطار تنفيذ معالجة البيانات بصورة غير قانونية (أ)، أو من خلال التعسف في استخدامها (ب).

أ- المعالجات الاحتيالية للبيانات.

الأنشطة التي تنطوي على تنفيذ المعالجة الآلية للبيانات الشخصية ليست فقط قانونية، بل لازمة لحسن سير و عمل مجتمع المعلوماتية والاقتصاد الرقمي. ونظرا لأهمية القضايا المتعلقة بسرية تلك البيانات، فإن معالجة البيانات الشخصية يخضع لإجراءات صارمة يترتب عن عدم احترامها فرض عقوبات جزائية. وهكذا فإن الأفعال الاجرامية الالكترونية المتعلقة بمعالجة البيانات الشخصية هي أفعال لا يحترم من خلالها مسؤولي المعالجة القواعد التي تفرضها النصوص

---

http://www.cyberoam.com/downloads/ThreatReports/CyberoamCYRENInternetThreats2014April.pdf.

المذكورة أعلاه. القواعد التي تفرضها النصوص المذكورة أعلاه. إن المساس بحقوق الأشخاص الناجمة عن الملفات أو عن المعالجة الآلية للبيانات في الجزائر مجرم من خلال المواد 394 مكرر – 394 مكرر7 من قانون العقوبات. تنطبق نفس القواعد و نفس الجرائم على الأشخاص المعنوية (394 مكرر4 ق.ع).

على المستوى الأوروبي اقتصر التوجيه رقم 95/46 على النص أنه "تتخذ الدول الأعضاء التدابير المناسبة لضمان التنفيذ الكامل لأحكام هذا التوجيه وعلى وجه الخصوص تحديد العقوبات التي ستطبق عند مخالفة الأحكام المقرّرة وفقا لهذا التوجيه "(المادة 24)، و إن مقترح التنظيم واضح إلى حد كبير حول العقوبات المطبقة عند عدم احترام الالتزامات المتعلقة بمعالجة البيانات الشخصية. يمكن تقسيم هذه الالتزامات إلى فئتين: تلك المتعلقة بجمع البيانات وتلك المتعلقة بأمن المعالجة الآلية لها.

ب- إساءة استخدام البيانات.

إن البيانات التي تدخل في بناء الهوية الرقمية للشخص تتمثل من جهة في الآثار الرقمية التي يتركها عند ممارسة نشاطاته على الانترنت، و من جهة أخرى في التسجيلات التي تقوم بها مختلف أدوات المراقبة الرقمية. إن المخاطر الرئيسية المرتبطة بسوء استخدام هذه المعلومات تتمثل أولا في سرقتها التي قد تساهم في قيام جريمة انتحال الهوية ثم ثانيا في استخدامها في إطار التسويق التجاري الذي يأتي في ظروف لا تفي بالتزامات اعلام ورضا الشخص المعني.

بخصوص المخاطر المتعلقة بجريمة انتحال الهوية ودون أن يكون هناك تعريف دولي محدد لهذه الجريمة، يمكن اعتبار سرقة هوية الشخص في الحصول و استعمال عن طريق الغش للمعلومات الخاصة به. وهكذا فإن انتحال الهوية على الانترنت تعتبر بمثابة انحراف عند ممارسة حرية التعبير على الإنترنت. ونظرا لغياب طرق تعريف موثوق بها على الشبكات الرقمية، سرعان ما أصبح من السهل انتحال هوية شخص آخر. إن تطور خدمات التجارة الإلكترونية و

الخدمات الرقمية المشروط بالأمن و ثقة المستخدمين[1]، من المحتمل أن يتعثر في مواجهة مخاطر انتحال الهوية الرقمية و اعادة استخدامها بشكل لا يمكن التحكم فيه. بالنظر إلى تفاقم هذه الجريمة، اعتمدت بعض الدول تشريعات بهدف ردع سرقة الهوية في البيئة الرقمية.

أما بخصوص المخاطر المتعلقة بعدم احترام حقوق الأشخاص من طرف مقدمي الخدمة في إطار بيع البيانات الشخصية. في الواقع وبالنظر إلى الممارسات في هذا المجال وخاصة تلك المتبعة في الولايات المتحدة الأمريكية (اجراء discovery[2])، هناك مخاوف جدية من جانب السلطات الأوروبية المسؤولة عن حماية البيانات، إضافة إلى الكشف عن خطر المراقبة الجماعية والدخول عن طريق الغش في أنظمة تخزين البيانات. إن بيع البيانات الشخصية الخاصة بمواطني الاتحاد الأوروبي لصالح الشركات الخاضعة لقانون الولايات المتحدة (مع العلم أيضا أنه في بعض الظروف يطبق خارج أراضيها، مثل قانون باتريوت آكت أو قانون مكافحة الإرهاب) يزيد من خطر الجريمة على هذه

---

[1] Ruth Halperin, « Identity as an Emerging Field of Study », Datenschutz und Datensicherheit, 2006, p. 533.

[2] مما يتميز به القضاء الأمريكي والبريطاني إجراء قديم معروف يسمى في أمريكا بـــ "Discovery"ويعرف فى بريطانيا بـــ "Disclosure"ويمكن ترجمته بـــ"المكاشفة" أو "الإفصاح". وهذا المبدأ هو إجراء من إجراءات ما قبل المحاكمة ويقصد به أن لكل طرف من أطراف القضية –بقوة قانون المرافعات– الحق فى الحصول على جميع الأدلة والبيانات المتعلقة بالقضية من الطرف الآخر قبل بدء الترافع. ويشمل ذلك الاستجوابات، والوثائق، والشهادات وغيرها وفق أطر قانونية دقيقة منصوص عليها فى قانون المرافعات. وبعد إظهار جميع الأدلة للطرف الآخر تجمع ثم ترسل نسخة منها إلى المحكمة. ويهدف هذا الإجراء إلى أمرين: أ– أن كثيرا من القضايا تنتهي بالصلح عند هذه المرحلة بسبب ظهور أدلة قد يجهلها أحد الأطراف وتبين قوة أو ضعف مركزه القانوني.

البيانات بسبب سوء استغلالها من قبل الأمريكيين. يضاف إلى كل ذلك النتهاك الملاحظ للحقوق و المتصل ببرنامج PRISM[1].

2- الجرائم الماسة بالأصول غير الملموسة للأشخاص المعنوية.

وفي مواجهة تجريد الوسائط من طابعها المادي والتي تخزّن فيها بيانات الشركات والدوائر الحكومية، كان لابد من أن تتكيّف القواعد القانونية من أجل حماية فعّالة للبيانات. في هذا الاتجاه كان من المناسب أولا أن تكون سرية المهارات والسر التجاري الخاصة بالأشخاص الاعتبارية مضمونة بشكل فعال **(أ)**، وثانيا أن يكون فعل سرقة المعلومة معروف و مجرّم **(ب)**.

أ-المساس بالبيانات السرية الخاصة بالأشخاص المعنوية.

لا يملك الشخص المعنوي الذي يكون ضحية لانتهاك بياناته السرية الخاصة حاليا في النظام القانوني الجزائري إلا الطرق غير المباشرة من أجل تأسيس شكواه – من جهة يتعلق الأمر بالمبادئ المرتبطة بانتهاكات حقوق الملكية الفكرية (التقليد[2] والمساس بالسر المهني[3] والمنافسة غير المشروعة[4] أوالتطفل التجاري[5])،

---

[1] بريسم أو بريزم بالإنجليزية PRISM :برنامج تجسس رقمي مصنف بأنه سري للغاية يتم تطويره من طرف وكالة الأمن القومي الأمريكية (NSA) منذ عام 2007 . خول البرنامج وكالة الاستخبارية الأميركية اختراق الرسائل الالكترونية، والأحاديث الالكترونية الشات والمكالمات الصوتية وغيرها من الوثائق لأشخاص في الخارج وفي الداخل الاميركي. كشفت الوثائق المسرّبة أن NSA كانت قادرة على الدخول مباشرة إلى الخوادم الخاصة لكل من مزوّدي الخدمات الأميركية :مايكروسوفت، ياهو، غوغل، آبل، فيسبوك، يوتيوب، سكايب.

[2] المواد من 151 إلى 155 من قانون حقوق المؤلف و الحقوق المجاورة و 61 و62 من قانون براءات الاختراع و المواد من 26 إلى 33 من قانون العلامات.

[3] المادة 301 من قانون العقوبات.

[4] المادة 6 و 13 و 14 من قانون المنافسة.

[5] المادة 27 من قانون القواعد المطبقة على الممارسات التجارية.

ومن جهة أخرى من خلال نصوص رادعة لانتهاك سرية المراسلات وخيانة الأمانة والسرقة والنصب والدخول غير المشروع في نظام معلوماتي أو تعطيله، الإخفاء، المساس بالمصالح الأساسية للأمة، الخ[1]. تجدر الاشارة إلى أنه فقط بعض المعلومات السرية تكون معنية بالحماية المتعلقة بالالتزام بالسر المهني، و الذي يترتب عن الاخلال به التجريم المنصوص عليه في قانون العقوبات. لكن يبقى أن العديد من البيانات لا تدخل ضمن نطاق حماية هذا النص.

ب-سرقة المعلومة.

وعلى الرغم من تزايد قضايا سرقة الأشياء غير الملموسة، فإن الاجتهاد القضائي الحالي يرفض الاعتراف بمفهوم "سرقة المعلومات" على أساس المادة 350 من قانون العقوبات. بالفعل فإن السرقة باعتبارها "اختلاس تدليسي لملك الغير" لا تنطبق على الأشياء غير الملموسة – بما في ذلك البيانات الموجودة في الأنظمة المعلوماتية للشركات. في فرنسا تطورت الأوضاع في السنوات الأخيرة حيث أقرّت محكمة النقض الفرنسية في بعض القرارات بوجود جريمة سرقة البيانات المعلوماتية، ولا سيما في حالات النسخ البسيط للبيانات[2]، ولكنها لم تقتصر على ذلك فقط[3]. إلا أن المبدأ يبقى ثابتا: حيث تنطبق جريمة السرقة على

---

[1] للاطلاع على مجموعة من الحلول في القانون المقارن أنظر:
Francis Hagel, « Protection des secrets d'affaires: enjeux et repères », Cah. Dt. Entr. janv.-févr. 2012, n°3, p. 31 et s.

[2] Cass. Crim. 4 mars 2008, n°07-84.002 ; TGI Créteil, 11ème ch. corr., 23 avr. 2013, Ministère Public c/ Olivier L.

[3] Cass. Crim. 4 mars 2008, n° 07-84002, J-P. X. c/ Sté Graphibus: Le vol était constitué même si les données n'avaient pas été soustraites (en l'espèce, elles n'avaient été que copiées).

الأشياء المادية الحسّية القابلة للانتقال. بينما المعلومات غير قابلة للتملك[1]، إلا إذا لجأنا إلى تفسير واسع للمفهوم، وهو ما يتعارض مع مبادئ القانون الجنائي.

الجرائم العابرة للقارّات.

وتستخدم مصطلحات مختلفة لوصف أفعال النصب المعقّدة المتصلة بأنواع مختلفة من الجرائم المتعلقة بالاتصالات الإلكترونية. وتشكل أعمال الإرهاب الإلكتروني (أولا) والحرب الإلكترونية (ثانيا) مكان التقاء العديد من الجرائم المذكورة أعلاه.

أولا: الارهاب الالكتروني.

إن مفهوم الإرهاب الالكتروني من المواضيع التي برزت حديثا و الذي يبقى تحديدها معقدا. بشكل عام يتمثل في توسيع نطاق الأنشطة لبإرهابية بمعناها "التقليدي". و لم يظهر النقاش الحاد حول استخدام تكنولوجيا المعلومات والاتصالات من طرف الإرهابيين إلا بعد هجمات 11 سبتمبر 2001[2] حيث أشارت تقارير إلى استخدام الإنترنت من طرف أسامة بن لادن من أجل التحضير للهجمات. يتضارب اتجاهين في تعريف الارهاب الالكترونى: من يعتبر أنه يجب أن يشمل كل ممارسات الجماعات الإرهابية على الانترنت[3] و آخر من يعتبر أن

---

[1] أ. اسامة سمير حسين، الاحتيال الالكتروني – الاسباب والحلول، ط1، عمان، الجنادرية للنشر والتوزيع، 2011، ص120.

[2] Marco Gercke, « Cyberterrorism, How Terrorists Use the Internet », Computer und Recht, 2007, p. 62 et s.; U. Sieber, P.W. Brunst, « Cyberterrorism – the use of the Internet for terrorist purposes », Cons. E., 2008, p. 9-105.

[3] Le Cons. E., par exemple, mentionne le cyberterrorisme comme étant « l'usage d'Internet pour des objectifs terroristes ». Cette expression

المصطلح ينبغي أن يقتصر على نوع معين من الاعتداءات، أي تلك التي تستخدم الانترنت كسلاح و / أو كهدف. لذلك لا يزال بعض الفقه حذرا جدا في تحديد الإرهاب الإلكتروني على أنه "التقارب بين العالم المادي والعالم الافتراضي"[1] أو على أنه "التقارب بين الارهاب و الشبكة."[2] في هذا الاتجاه يظهر الإرهاب الإلكتروني على أنه ببساطة نقل الأنشطة الإرهابية إلى العالم الرقمي. ومع ذلك يغامر آخرون في تفصيل هذا المفهوم من خلال اقتراح تعريف للارهاب الالكترونى على أنه "اعتداء عمدي وذو دوافع سياسية ضد المعلومات، والنظم المعلوماتية والبرمجيات والبيانات، ينتج عنه عنف ممارس ضد أهداف غير مقاتلة"[3]. هذا التعريف تم تبنيه من طرف مكتب التحقيقات الفدرالي الأمريكي FBI[4]. وهكذا يظهر عنصرين أساسين ينبثقان عن هذه التعاريف وهي "العنف"

---

demeure, cependant, très large et permet, en conséquence, l'émergence d'interprétations controverses – comme celle par le service de recherche du Congrès américain, pour lequel l'achat en ligne d'un billet d'avion pour les Etats-Unis par un des terroristes constitue une preuve que les terroristes ont utilisé Internet pour préparer leurs attaques, v. Clay Wilson, in CRS Report, « Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress », 2003, p. 4.

[1] Barry Collin, « The Future of CyberTerrorism: Where the Pysical and Virtual Worlds Converge », 11th Annual International Symposium on Criminal Justice Issues, 1996.

[2] Patrick Chambet, « Le cyber-terrorisme », adresse: http://www.chambet.com/publications/Cyberterrorisme.pdf.

[3] Benoît Gagnon, « Les technologies de l'information et le terrorisme, Repenser le terrorisme. Concept, acteurs réponses », Les presses de l'université Laval, 2007, p.260.

[4] Bonnie N. Adkins, « The spectrum of cyber conflict from hacking to information warfare: what is law enforcement's role? », Air Command

كنتيجة لهذه الأفعال و"أهداف غير مقاتلة" كضحايا لها. يتعلق الأمر إذن بالاستخدام المتعمد لأجهزة الاعلام الآلي أو شبكات الاتصالات، كأسلحة أو أهداف، بهدف ممارسة العنف وإثارة الشعور بإرهاب السكان من غير المقاتلين بغرض الاضرار أو التأثير في الرأي العام أو الحكومي بأقصى قدر من التأثير.

إن عنصر الترهيب المتصل بالنشاط الإرهابي بشكل عام يتفاقم عند استخدام الأدوات الرقمية. بالفعل فإن فكرة أنه بامكان أعداء مجهولين أن يحاولوا اختراق أنظمة المعلوماتية من أي مكان في العالم أحدث قطيعة مع التصور التقليدي للأمن – أين تكون هوية و موقع و أهداف العدو غالبا معروفة – ويزيد من الشعور بالخوف وانعدام الأمن. وبالإضافة إلى ذلك فإن الهجمات الإلكترونية تتميز بأنه من الصعب جدا تحديد الجهات التي تقف وراءها حيث يتم استخدام أسلوب متقدم يعتمد على عدة شبكات من أجهزة روبوتية BotNet. لا يمكن بأي حال من الأحوال إذن أن نثق كليا في مراسلات تبدو آمنة والتي من المحتمل أن تصدر من أجهزة حاسوب خرجت عن سيطرة مستخدمها الشرعي.

ثانيا: الحرب الالكترونية.

إن "الحرب الإلكترونية" مفهوم إشكالي للغاية، بعيد عن فكرة الحرب التقليدية ويخلو من استقلالية حقيقية. على المستوى العسكري الحصري يتعلق الأمر أساسا باضافة فضاء رقمي لعمليات مخطط لها في مجالات أخرى. وهكذا فإن "الحرب الإلكترونية" تتمثل في إعداد و توصيل و تضخيم، أو حتى تبديل بالنسبة لبعض الفقه: عمل القوات المسلحة بهجمات إلكترونية ضد أجهزة عسكرية، حكومية (سياسية أو إدارية)، وكذلك ضد القطاع الخاص. و هو نتيجة لعملية الرقمنة لساحة المعركة بين مختلف القوى.

---

and Staff College, Air University, avr. 2001, p. 11, adresse: http://www.au.af.mil/au/awc/awcgate/acsc/01-003.pdf.

يشير الكتاب الأبيض للدفاع الوطني الفرنسي لسنة 2013 إلى "الحرب المعلوماتية" و يصنفها ضمن قضايا الأمن القومي، وأكد على ضرورة انه على فرنسا أن تتزود بوسائل الهجوم المضاد (وليس فقط للدفاع والأمن).

ومع ذلك تتنوع الهجمات الالكترونية و لا تتطلب جميعها ردا عسكريا. عبارة "الحرب الإلكترونية" ينبغي أن تقتصر على الهجمات الأكثر خطورة التي تمس بأمن الدولة أو مصالحها الأساسية، لأنها تهديدات تستدعي ردا حكوميا مناسبا.

إلا أن خصوصية الأسلحة التي يمكن استخدامها أثناء هجوم الكتروني تكمن في أنها وخلافا لغيرها من التكنولوجيات مثل الطاقة النووية ليست حكرا فقط على الدول. إن الإرهابيين الإلكترونيين في كثير من الأحيان هم أشخاص يأتون من كتائب متفرعة عن المجموعات الإرهابية التقليدية. ويمكن لهم أن يكونوا في جماعات منظمة أو أن يتصرفوا دون تنظيم معين، مع أهداف ومخططات متفاوتة التحديد، ويتمتعون بمهارات تقنية متطورة على نحو متزايد. تتحصر ضحايا هذه الهجمات التي تطال اقتصادات بأكملها وتهدد الأمن القومي: في الدول (البنية التحتية ومصالح الجيش) والشركات (مقدمي الخدمة، ومتعاملي التجارة الإلكترونية، إلخ).

وفي هذا السياق تفرض الحرب الإلكترونية تحديات خاصة فيما يتعلق بالبنية التحتية الحيوية التي يترتب عن تعطيلها أو تدميرها، إضعاف الدفاع أو الأمن الاقتصادي للدولة[1].

---

[1] « Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve », GAO communication, juill 2007, adresse: http://www.gao.gov/new.items/d07706r.pdf.

وعلاوة على ذلك وما دامت الحرب الإلكترونية شكلا من أشكال الصراع المسلح المبني على إدارة واستخدام المعلومات بجميع أشكالها وعلى جميع الأصعدة لنيل مكسب عسكري حاسم، وتشكل المعلومات في هذا الاطار رصيدا قيّما وأداة غزو أودمار، والتي تكون سلامتها وسريتها مهددة بأعمال متعلقة بالتجسس الصناعي.

تجدر الاشارة في الأخير أن الهدف النهائي يتمثل في إيجاد توازن بين تطبيق قواعد حفظ النظام العام وأمن الأشخاص – بالضرورة من خلال تقييد معين للممارسة المطلقة للحريات العامة وبين الحفاظ على هذه الأخيرة إلى أقصى حد ممكن.

القيود التي تفرضها المراقبة الرقمية على حرية التعبير والاستخدام الحر للانترنت.

هناك قيود مختلفة قد تؤثر على حرية الأفراد في الاتصال ونشر المحتوى الرقمي الذي يختارونه (فرع أول) و قد تؤثر أيضا على الوصول إلى الشبكة، وإلى مختلف المحتويات والوسائل والتي يمكن استخدامها – خاصة حرية استخدام أدوات تشفير الاتصالات (فرع ثاني).

تأمين شروط بث المحتوى الرقمي في مواجهة احترام حرية التعبير والاتصال.

إن مختلف القيود على النشر الحر للمحتوى الرقمي (أولا) يجب أن تتكيف حتى لا تتسبب في المساس بالحريات العامة للأشخاص وأن لا تثير الشك أو توحي بأفكار خاطئة حول وظيفة الانترنت (ثانيا).

أولا: القيود على نشر المحتوى الرقمي المجرّم.

القيود المفروضة على تصفح المحتوى الرقمي تبررها ضرورة ضمان الأمن والنظام العام وفرض احترام الآداب العامة من جهة (أ) وحماية الحقوق الأساسية بما في ذلك الحق في الملكية من جهة أخرى (ب).

أ- القواعد التي تفرض قيودا على نشر المحتويات المجرمة.

إن الهدف من تدابير اعتراض أو حذف بعض المحتويات يتمثل في الحد من وجود المواد غير المشروعة في الشبكات الرقمية. على سبيل المثال يمكن اعتراض بريد إلكتروني باعتباره بريد مزعج، قد يتم حظر موقع على شبكة الانترنت لاحتوائه على برامج ضارة أو شبكات الند للند (" *peerto-peer* ") يمكن توقيفها بسبب الاشتباه في نقلها لمحتوىات تتعلق بالميول الجنسي للأطفال. إن المحتويات ذات الصلة يمكن أن تكون مدونات جهادية، منشورات على الشبكات الاجتماعية، فيديوهات ذات طابع عنصري أو عنفي أو إباحي متعلق بالميول الجنسي للأطفال وتكون منشورة على المنصات أو على منتديات المناقشة، الخ.

إن تدابير حجب المحتويات المسيئة ضرورية للحفاظ على النظام العام. ويتم ذلك من خلال طريقين: طريق قضائي وآخر إداري. في الحالة الأولى يكون الحجب تحت إشراف القاضي، في حين أنه في الحالة الثانية يعتمد على صدور قرار إداري. بالنسبة للحجب القضائي للمحتوى غير القانوني هو إجراء تبنته عدة دول[1]. المقاربات التقنية، والهدف من التصفية، فضلا عن درجة إشراك المتعامل الصناعي، كلها متغيرات متفاوتة. عموما يتم إرسال أوامر لمقدمي الخدمة الوطني ولكن غالبا ما تشمل أيضا الوصول إلى مواقع الانترنت المستغلة في

---

[1] من بين هذه الدول بصفة خاصة: إيطاليا ورومانيا وفنلندا وبريطانيا وأستراليا وأخيرا تركيا.

الخارج. في بلجيكا على سبيل المثال يحق لقاضي التحقيق أن يأمر مقدمي الخدمة بإيقاف خدماتهم في حال وجود خطر على السلامة العامة والأمن الوطني والدفاع الوطني أو على مصلحة المستهلك[1]. بخلاف ذلك في الولايات المتحدة الأمريكية لا يوجد نظام إلزامي بالتصفية، باستثناء ما تفرضه الدولة على المدارس والمكتبات، حيث أنه وللاستفادة من تخفيض سعر خدمة الإنترنت يجب عليها اتخاذ تدابير تصفية المواد العنيفة أو الإباحية الماسة بالطفل[2].

وفيما يتعلق بالحجب الإداري الذي يظهر كإجراء مثير للجدل لأنه يشكل تعد على دور القاضي في عملية حجب المحتوى. وهو تجسيد نوعي لتنفيذ اجراء من اجراءات الضبط الإداري في مواجهة نشاط ماس بكرامة الإنسان. ولتبريره يستشهد أنصاره بدوره في ردع الإخلال بالنظام العام والأمن والأخلاق والآداب العامة بشكل أسرع وأنجع.

الطريقة الأكثر وضوحا لتجسيده تتمثل في تحديد هيئة حكومية لقائمة من عناوين مواقع الانترنت التي يجب أن يتم حجبها من طرف مقدمي خدمات الإنترنت. في أستراليا على سبيل المثال فإن مثل هذه القائمة السوداء ("*block–list*") يتم إنشاؤها من طرف الهيئة الأسترالية للاتصالات والإعلام (ACMA)،

---

[1] Thomas Weigend, « Rapport général sur la société de l'information et le droit pénal au XIXème congrès de l'Association internationale de droit pénal », Revue internationale de droit pénal, 2013/1, vol.84, p. 19-47, adresse:
http://www.penal.org/sites/default/files/files/SECTION%20I%20General%20Report%20FR.pdf.

[2] وقد نص على ذلك قانون حماية الطفولة على الانترنت الصادر في سنة 2000 Children's Internet Protection Act (CIPA). أنظر الموقع:
http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/cipa/cipatext.pdf.

ملزمة لجميع مقدمي خدمات الإنترنت. والتكنولوجيا المستخدمة هي BT Cleanfeed، أي تكنولوجيا مبنية على تصفية عناوين مواقع الانترنت. في الدنمارك يتم إنشاء القائمة السوداء من طرف المركز الوطني لمكافحة الجرائم المتصلة بالتكنولوجيات الحديثة ("*National High Tech Crime Centre*") ا التابع للشرطة الوطنية الدنماركية، ومن طرف مكتب المساعدة على الانترنت " *Save the Children Denmark* ". يتم حجب المواقع الواردة في هذه القوائم دون حكم قضائي.

ب- حماية حقوق الملكية الفكرية.

إن حماية الملكية الفكرية مفهوم معترف به ومطبق عالميا، بما في ذلك في البيئة الرقمية. ومع ذلك فإن حقوق الملكية الفكرية كأي حق آخر ليست مطلقة، ويجب أن تتعايش مع الحقوق الأساسية الأخرى والتقنيات الرقمية التي تعيد النظر في مفهوم الملكية، بتمييع قيمة الأصول غير الملموسة. والأمثلة كثيرة في مجال حقوق المؤلف، حيث غالبا ما ينظر إلى العمل ليس بوصفه مصنف مبتكر من طرف المؤلف، ولكن كمعلومة تستوجب النشر. في هذا السياق فإن ردع انتهاكات حقوق المؤلف والحقوق المجاورة يثير استياء المجتمع المدني الرقمي على نحو متزايد لأنه يؤدي إلى زيادة الرقابة على جميع مستخدمي الإنترنت. وقد أثرت هذه الظاهرة أيضا على الجهات الفاعلة في الاقتصاد الثقافي التي بدأت في تطوير بدائل تحت المصطلح العام "البيع القانوني" والتي تساهم في تطوير نماذج اقتصادية جديدة، مثل "التمويل الجماعي crowd founding".

تجدر الاشارة في الأخير إلى وجود نزاع حقيقي بين أصحاب الحقوق المجاورة والمواطنين المعتادين على نحو متزايد على مجانية المصنفات ويعارضون بشكل متزايد احتكارها.

ثانيا: أخطار الاختلال أو المساس بالحقوق والحريات من خلال التدابير المقيّدة.

إن مسألة تصفية أو فلترة وحجب مواقع الانترنت تؤثر بشكل مباشر من جهة على العراقيل التقنية التي تميّز الشبكات الرقمية (1) وعلى احترام الحريات العامة للأفراد والضمانات الرئيسية التي تأمن شرعية القواعد المطبقة على الانترنت من جهة أخرى (2).

1- الصعوبات التي تواجه تطبيق إجراءات التصفية.

يمكن تبادل المحتويات الرقمية بواسطة تكنولوجيات مختلفة. لذلك فإن تصفية عدد محدود منها (كالاكتفاء بتصفية حركة المرور نحو خوادم الانترنت فقط) يمكن أن يؤدي إلى استعمال طريقة أخرى في توزيع المحتوى. إن الذين يريدون توزيع المواد غير الشرعية عبر شبكة الإنترنت لديهم جملة من الخيارات للقيام بذلك، على الرغم من تدابير التصفية المطبقة. لا يوجد مصفاة ناجعة بشكل كامل، حيث يجب الأخذ بعين الاعتبار حقيقة أن التزام المضيف هو التزام ببذل عناية، وأنه يجب استباق عواقب أي أخطاء ممكنة عند إزالة المحتوى والالتزام بالضمانات الضرورية لاحترام حقوق مستخدمي الانترنت (الحق في الاعلام المسبق، والحق في الاعتراض، إلخ)[1]. بالاضافة إلى ذلك يجب اعادة النظر وذلك بتطوير نظام التصفية الحالي، و المبني على أساس قوائم الكلمات الرئيسية أو العناوين المحددة مسبقا، وهو نظام يبقى غير فعّال ويستدعي إجراء تحديثات

---

[1] Alexandra Neri, « L’injonction de filtrage rendue à l’égard d’un intermédiaire: une mesure controversée aux conséquences redoutables », op.cit.

منتظمة[1]. على أي حال، واحدة من أهم الصعوبات التي تواجه الجهات الفاعلة التي تريد السيطرة على تدفق البيانات على الأقل تتمثل في لا مركزية الخوادم التي تتدفق من خلالها هذه البيانات وأيضا في الطابع العابر للحدود للشبكة. في كثير من الأحيان يكون المحتوى غير القانوني – وهذا ينطبق بشكل خاص على تلك المتعلقة بالمواد الإباحية الخاصة بالأطفال – متاحا على مواقع الانترنت المستضافة في دول تكون تشريعاتها اباحية مقارنة بالمعايير الدولية. وتكون كذلك إجراءات الإخطار وحجب المحتوى في هذه الدول متخلفة أو لا تعمل. ولذا قد تكون مهمة الاتصال بمتعاملي القطاع في هذه الدول معقدة بشكل خاص ويكون أكثر تعقيدا مطالبتهم بالالتزم باجراءات الحظر المطبقة في أوروبا أوفي الولايات المتحدة على سبيل المثال.

2- القضايا الرئيسية المتعلقة بتدابير التصفية.

إن طبيعة ونطاق والأثر الكبير الذي يمكن لتدابير التصفية أن تشكله على حقوق وحريات مختلف الأطراف المعنية، يدعو الى تحليل عميق وأخذ احتياطات جدية. ومن المهم الاشارة إلى الطبيعة التطفلية للعديد من إستراتيجيات التصفية. تظهر هذه الحقيقة بشكل خاص فيما يتعلق بآليات التصفية الدقيقة للمحتوى، والتي تتطلب تحليل المحتوى المتبادل بين المستخدمين. في جميع الحالات يجب تقيّيم شرعية التدابير الآمرة بمدى احترامها لالزامية حماية الحريات الأساسية، وهي

[1] Mathieu Valette, « Détection et interprétation automatique de contenus illicites et préjudiciables sur internet: un exemple de sémantique textuelle appliquée: le projet PRINCIP », adresse: http://faculty.arts.ubc.ca/winder/me/linguistique_du_corpus/Valette_PRINCIP.html.

المقاربة الوحيدة الممكنة في ظروف أصبح فيها من الصعب بشكل خاص الوصول إلى توازن بين مختلف الحقوق والمصالح المعنية. بالفعل فكلما تم الترخيص لتدبير من تدابير التصفية لفعّاليته في الحفاظ على مصلحة مشروعة، فإنه لا ينبغي أن يحد من الحريات الأخرى على نحو غير متناسب، وأن تؤطره ضمانات معينة بحيث لا يتم استخدام هذا اتدبير بطريقة يمكن أن تهدد هذه الحريات. لهذا السبب لا يمكن للقضاة صرف النظر عن العواقب الملموسة التي يمكن أن تنتج عن تنفيذ التدابير الآمرة.

وعلاوة على ذلك فإن تصفية المحتوى في قلب النقاش العالمي[1] لأنه كما يتعارض بالضرورة مع مبدأ الحياد الملازم لفكرة شبكة الانترنت، يعرّض أيضا للخطر مبدأ الفصل بين السلطات من خلال تجريد القاضي من دوره الرقابي، أو لأنه يشكل خطر تسريب أدوات التصفية لصالح جهات خاصة.

تأمين شروط استخدام الانترنت أمام حرية الوصول إليها والتشفير.

قد تخضع حرية الوصول إلى الانترنت لبعض القيود تبررها نية المشرع لتأمين المراسلات الرقمية. وهكذا فإن الوصول إلى الشبكة نفسها أو الوصول إلى محتوى معين من طرف فئات معينة من الأشخاص قد يكون مقيدا (أولا). وبالمثل ومن دون تقييد استخدام الانترنت وفي ظروف معينة فإن حق الأشخاص في استخدام تقنيات التشفير لجعل مراسلتهم سرية يمكن أن يكون موضع تساؤل (2).

[1] Antonino Troianiello, « La CJUE s’oppose au filtrage généralisé de l’internet », RLDI 2012/78, n°2613.

أولا- تقييد الوصول إلى الشبكة والمحتويات الرقمية.

في إطار مكافحة نشر المحتوى غير القانوني أو الضار، يتدخل المشرع لردع من جهة، الوصول إلى الشبكة وإلى البيانات من طرف فئة معينة من الأشخاص (1)، ولتجريم التصفح المعتاد لهذا النوع من المحتوى (B).

1- التقييد المفروض على فئات معينة من الأشخاص.

إن التدابير المتخذة بهدف تقييد الوصول إلى شبكة الانترنت قد تنتج من جهة، عن الارادة في حماية الأشخاص المعرضين للخطر مثل الأحداث، وفي ردع الجرائم المرتكبة من جهة أخرى. في الحالة الأولى يتعلق الأمر بتقييد الوصول إلى أنواع معينة من المحتوى التي تعتبر غير ملائمة بالنسبة إلى فئة الأشخاص المعنية وفي الحالة الثانية يكون الاعتراض على مستوى الاشتراك في شبكة الإنترنت، وبالتالي اعتراض الوصول إلى خدمة الاتصالات العامة على الانترنت.

2- تجريم التصفح المعتاد للمحتوى غير المشروع.

إن التدابير المتخذة بهدف تجريم مشاهدة مستخدمي الإنترنت للمحتوى غير المشروع جاءت مكملة لتلك التي تستهدف نشره. وخلافا لحجب المحتوى غير المشروع المتعلق بالجانب الجزائي، يجب النظر إليها من الجانب الوقائي. بالفعل يعتبر هذا المكمل ضروريا لتعزيز مكافحة الإرهاب والاعتداء الجنسي على الأطفال، بالنظر من جهة إلى العراقيل التقنية المتصلة بإزالة المحتوى غير المرغوب فيه في الشبكة الرقمية، و ضرورة العمل أكثر من أجل الحد من السلوكات المنحرفة اللاحقة من جهة أخرى.

يرتبط تجريم التصفح المعتاد للمواقع ذات الطابع الإرهابي والتي يكون موضوعها الاستغلال الجنسي للأطفال في الواقع مباشرة بإعداد وتمويل هجمات

إرهابية وتجنيد الإرهابيين وتطوير شبكات الاستغلال الجنسي للأطفال. عند متابعة الأشخاص الذين يدخلون بانتظام المواقع المعنية، يأمل المشرع في امكانية تجنب التطرف المحتمل لأفكارهم أو التورط مستقبلا في أعمال إجرامية. على سبيل المثال، فيما يتعلق بالإرهاب، نشهد حاليا ظاهرة التطرف الذاتي، الذي أصبح ممكنا من خلال المواقع الإلكترونية التي تدعو لارتكاب أعمال إرهابية وتوفر طرق ارتكابها. أصبحت النظم القانونية البريطانية والألمانية، جنبا إلى جنب مع النظام الفرنسي على بينة من هذه المسألة، حيث تتطرق إلى فكرة المشروع الإرهابي الفردي.

ثانيا: تقييد استخدام وسائل التشفير.

هناك دوافع متعددة تجعل الدول تفرض قيودا في مجال التشفير – يتعلق البعض منها باستيراد وتصدير تكنولوجيات التشفير (1)، والبعض الآخر باستخدام وسائل التشفير على أراضيها (2).

1- القيود المفروضة على استخدام تكنولوجيات التشفير.

تتوجس حكومات العالم لفكرة أنه بامكان مواطنيها من ممارسة حقهم في حياة خاصة من خلال التواصل دون أن تكون السلطات العمومية قادرة على فك تشفير محتوى المراسلات[1]. و تبرر هذه القيود بضروريات الدفاع الوطني وأمن الدولة.

---

[1] أنظر بخصوص هذه النقطة:

Bruce Sterling, « The new cryptography », The Magazine of Fantasy & Science Fiction, n° 12, adresse: https://w2.eff.org/Misc/Publications/Bruce_Sterling/FSF_columns/fsf.12 ; Abderrahmane Nitaj, « La cryptographie et le confiance numérique », 23 mars 2013, adresse: http://www.math.unicaen.fr/~nitaj/cryptoconfiance.pdf.

في الصين على سبيل المثال، يخضع استيراد وتصدير التكنولوجيا التشفير إلى درجة عالية من التنظيم. وقد تم وضع نظام للتراخيص والتصاريح من أجل السيطرة على أي نشاط في هذا المجال على المستوى الحكومي. والنتيجة هي أن الشركات والأفراد لا يمكنها استخدام إلا وسائل التشفير التي حصلت على ترخيص من طرف الدولة.

على خلاف ذلك فإنه في الولايات المتحدة الأمريكية، والتي تأتي منها معظم تقنيات التشفير، هناك قيود قليلة على استخدامها. و تعود الموجودة إلى زمن الحرب الباردة وتهدف لتحقيق التوازن بين مسألتين: تعزيز القدرة التنافسية للصناعة الأمريكية في الأسواق الخارجية، والحد من قدرة المجرمين والإرهابيين على تعريض الأمن القومي من خلال استخدام وسائل تشفير قوية. وتجدر الاشارة أنها تقتصر على نشاطات تصدير التكنولوجيا – أما ذات الاستخدام الشخصي أو المستوردة فهي مباحة و بدون قيود – ويشكل ذلك قاسما مشتركا مع النظام المعمول به في الاتحاد الأوروبي.

ينظم الاتحاد الأوروبي تدفق تقنيات التشفير عن طريق اللائحة الأوروبية رقم 2009/428 بإنشاء نظام أوروبي للرقابة على الصادرات ونقلها والسمسرة وعبور البضائع ذات الاستخدام المزدوج[1]. يخضع هذا النص إلى جانب التكنولوجيا النووية والمواد الحربية إلى ترخيص: تصدير "النظم والمعدات، المركبات الإلكترونية الخاصة بتطبيق معين، وحدات ودوائر متكاملة (...) المصممة أو المعدلة لاستخدام "التشفير" تعتمد على تقنيات رقمية تؤدي وظيفة التشفير باستثناء المصادقة أو التوقيع الرقمي "، ويشمل نظام التصاريح أيضا تقنيات التشويش. ومع ذلك لا تخضع لأي ترخيص البرمجيات "التي هي في

---

[1] JO L 134 du 29 mai 2009, p. 1–269.

متناول للجمهور عادة" لأنها "تباع مباشرة من المخزن و بدون قيود"، سواء في محل ابيع، عن طريق البريد أو عن طريق المعاملة الالكترونية. بالتالي فهي معفاة من نظام الترخيص برامج التشفير الالكتروني الموجهة للجمهور.

تم تخفيف القواعد الفرنسية المطبقة على استيراد وتصدير وتوريد واستخدام وسائل التشفير مع مرور الوقت. إلى غاية سنة 1999 كانت الحكومة تمارس سياسة حظر غير مباشر لاستخدام وسائل التشفير، والآن توقفت عن اشتراط ترخيص من أجل استيراد تكنونلوجيات التشفير، واستبدلته بمجرد تصريح بسيط.

فيما عدا القواعد التي تنظم استيراد وتصدير تكنولوجيات التشفير، قد يتم فرض قيود أخرى – وهذا حتى في البلدان التي تعتبر أكثر ليبرالية في هذا المجال – للجعل من الممكن الوصول إلى البيانات لغرض التحقيق القضائي أو للحفاظ على الأمن القومي.

2- القيود المفروضة على قدرة الأشخاص في تشفير اتصالاتهم.

تهدف رقابة الدول على عمليات التشفير إلى منع المساس بالأمن الداخلي والخارجي للدولة. بالفعل حرية استخدام وسائل التشفير لا ينبغي أن تستخدم لإحباط مقتضيات العدالة في سياق التحقيقات الجنائية أو الإرهابية أو الإدارية في مواد الاعتراض والتنصت[1]. تختلف القيود بين منع تشفير الملفات والتزام المستخدمين في الكشف عن كلمات السر ومفاتيح التشفير أمام الهيئات القضائية المختصة. وكمثال لدولة قامت بفرض المنع الشامل للتشفير على أراضيها هي باكستان. بلدان أخرى تنص على سبيل المثال على التزام كشف البيانات، ولكنه غير نافذ في مواجهة المتهم أو عائلته (وهذا هو الحال في بلجيكا على سبيل المثال). بالفعل فإنه يجب تحليل التزام كشف البيانات في ضوء الطابع الماس

---

[1] أنظر بصفة خاصة قانون الأمن الداخلي: المواد L. 241-1 و s.

بالحق في عدم تجريم الذات ("*right against self-incrimination*") والحق في التزام الصمت ("*right to silence*").

في الولايات المتحدة الأمريكية ينص البند الخامس على الحق في عدم تجريم الذات وأصبح ينظر إليه كعقبة لطلب السلطات في تزويدها بالمحتوى المشفر. حتى ذلك الحين وعلى الرغم من اقرار المحاكم أنه حتى في اطار تحقيق جنائي، ليس هناك أي التزام للكشف عن مفتاح فك التشفير[1]، إلا أنها وافقت على الأمر بفك تشفير البيانات[2]. ولكن مع قرار صدر مؤخرا من محكمة إستئناف[3]، بدأ القاضي الأمريكي ربما في دعم حماية سرية الاتصالات واحترام الحق في عدم تجريم الذات، على حساب وصول السلطات العمومية إلى المحتوى المشفر.

جاء في تقرير توضيحي لاتفاقية الجريمة الإلكترونية لمجلس أوروبا أن "تعديل البيانات لحماية الاتصالات (التشفير على سبيل المثال)" يعتبر شرعيا لأنه يسمح بضمان "حماية مشروعة للحياة الخاصة". ولكن تنص الاتفاقية في المادة 18 على أنه بإمكان الدول الموقعة إجبار الأشخاص المقيمين داخل أراضيها على تقديم البيانات كما حددت ترتيبات معينة بشأن شكل البيانات المقدمة: "النص دون التشفير، على الانترنت، مطبوع أو على قرص مرن". هذه الصيغة تدخل في

---

[1] Federal Discrict Court of Vermont, In re Grand Jury Subpoena to Boucher, 2007 WL 4246473, 29 nov. 2009.

[2] United States c/ Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012).
في هذه القضية، في حين تم التأكيد على أن المشتبه فيه لا ينبغي أن يضطر إلى أن يكشف للسلطات الأمنية عن كلمة المرور التي تمنع الوصول إلى القرص الصلب لجهاز الكمبيوتر الشخصي، اعتبر القاضي أن البند الخامس الذي يحمي ضد التجريم الذاتي autoincriminationلا يمنع السلطات من طلب تقديم نسخ عن المحتوى الموجود في نسخة غير مشفرة.

[3] 11th Circuit fot the US Court of Appel, United States c/ Doe, 24 févr. 2012, n° 11-12268, 11-15421.

اطار سياسة المجلس الأوروبي في مجال عرقلة سير الإجراءات الجزائية بسبب استخدام تكنولوجيات المعلومات[1].

في بريطانيا يضع الباب الثالث من قانون تنظيم سلطات التحقيق لسنة 2000 قواعد محددة تطبق في اطار الإجراءات الجزائية لإجبار المتهم على فك تشفير بياناته واتصالاته. ثلاث فرضيات لهذا الأمر القضائي منصوص عليها في المادة 49: لمقتضيات الأمن القومي لمنع أو كشف جريمة أو للمصلحة الاقتصادية للبلد. وتكون العقوبة[2] الحبس من سنتين أو خمس سنوات عندما يتعلق الأمر بالأمن القومي (على وجه الخصوص في اطار مكافحة الإرهاب أو المواد الإباحية المتعلقة بالاستغلال الجنسي للأطفال).

ولفرنسا أيضا ترسانة قانونية مقيّدة للغاية عندما يتعلق الأمر بالتزام فك البيانات المشفرة. والاختلاف مع الأنظمة الأخرى يكمن في أنه ليس هناك أي التزام مباشر لتقديم البيانات بعد فك تشفيرها بأمر من السلطات المختصة وفك التشفير لا يكون إلا عن طريق مقدم الخدمة المعيّن خصيصا للقيام بهذا الاجراء (230-1 إلى 230-5 اج).

---

[1] A propos de l’utilisation des techniques de chiffrement, dans la rec. n° R (95) 13, le Conseil estime que « Des mesures devraient être examinées afin de minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales, sans toutefois avoir des conséquences plus que strictement nécessaires sur son utilisation légale. », v. p. 14 , adresse:
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900873&SecMode=1&DocId=527814&Usage=2.

[2] Regulation of Investigatory Powers 2000 c. 23, Part III, Offences, Section 53.

جميع التدابير التي تم تحليلها أعلاه تهدف للحد من الآثار السلبية لاستخدام التشفير على مجرى التحقيقات الجنائية. القضايا المتصلة بتنفيذ هذا النوع من التدابير تبقى بالرغم من ذلك مهمة وذلك لأنه يشكل تدخلا من السلطة العامة في ممارسة الحريات الأساسية لأشخاص – حرية الاتصال، بما في ذلك الذي يتم بصفة سرية. في حين أن انتهاك هذه السرية التي يكفلها التشفير يمكن تبريره في حالات حماية الأمن الوطني، متابعة مرتكبي الجرائم أو حماية المصالح الاقتصادية للدولة، فإنه يجب ضمان أن لا تستخدم هذه الامتيازات بطريقة تتعدى حالات الضرورة القصوى. يجب أن يظل فك تشفير البيانات استثناء وليس اجراء يستخدم عادة وفقا لتقدير الإدارة. يبرر الأمن التكنولوجي بالتأكيد اتخاذ الإجراءات المناسبة، ولكن وجود فائض من الحماسة في هذا الشأن يمكن أن يكون ضارا لعمل الانترنت، وتطوير التجارة الإلكترونية وحتى الأمن اليومي للمواطنين[1].

القيود التي تفرضها المراقبة الرقمية على الحق في حرمة الحياة الخاصة.

كما لاحظنا سابقا أصبحت الإنترنت مكانا للتبادل يستعمله المجرمون والجماعات الإرهابية بسهولة. و هذا لعدة أسباب مختلفة، بما في ذلك درجة عالية من السرية مرتفع مقارنة بالأعمال المرتكبة في العالم الحقيقي. وعلى الرغم من امتياز التستر الناشئ عن حقيقة أنه لا يطلب من مستخدمي الإنترنت تحديد هويتهم مسبقا عند استخدام الانترنت، إلا أنه كل عمل يترك آثارا قد تكشف عن

---

[1] Bertrand Warusfel, Franck Leprévost, « Cryptographie et lutte contre le terrorisme: éviter les fausses solutions sécuritaires », Droit et Défense, n° 2002/1, p. 17-22.

هوية المستخدم، تكون بالتالي قابلة للاستغلال من طرف أولئك الذين يرغبون في تحديد هويته (أولا).

وعلاوة على ذلك فإن آليات التحقيق التقليدية التي تعتمد على الاتصال الجسدي مع الشخص الذي يشتبه في ارتكابه الجريمة وعلى الوصول المادي إلى الأدلة، تبقى غير فعّالة أو حتى عاجزة أمام التستر النسبي للمستخدمين، ومجرمي الانترنت العابرين للقارات وتذبذب وسائل الاثبات المتاحة.

ولذلك فإن الأساليب الجديدة التي يتم تنفيذها من طرف السلطات العمومية تدخل في إطار سياسة القمع التي تواجه تحديات قانونية وتكنولوجية (ثانيا).

الدولة و تعقب الأشخاص على الانترنت.

من الضروري في مادة الاثبات الجزائي لحاجة التحقيق أن تتمكن مصالح الأمن من الحصول على بعض المعلومات حول الأنشطة التي تتم عن طريق الانترنت. في هذا الاطار يسعى المحققون من جهة لمعرفة موقع وهوية الجاني، والحصول والحفاظ على أدلة الاقناع من أجل اثبات الركن المادي للجريمة في مرحلة المحاكمة من جهة أخرى. وبالتالي فإن الدولة تسعى بطبيعة الحال إلى وضع تدابير للحفاظ على بعض من هذه الآثار واستخدامها في إطار الحفاظ على الأمن (أولا).

ولكن فيما عدا التمكن من الآثار التقنية، يتم تتبع الأشخاص أيضا من خلال أنظمة أنشئتها الدولة تسمح برصد بيانات الهوية وبيانات رقمية أخرى عن أنشطة المستخدمين (ثانيا).

أولا: المراقبة من خلال تتبع بيانات الاتصال.

من حيث المبدأ وبالنظر إلى الطابع التعريفي للبيانات، لا يجب الاحتفاظ بها من طرف مقدمي الخدمة التي تدير الوصول إلى الشبكة، ويتعلق الأمر بمتعاملي الهاتف النقّال ومقدمي خدمة الانترنت. لكن تنص معظم التشريعات ولأغراض

معينة تبرر ذلك، أن يتم الاحتفاظ بهذه المعلومات حسب الاقتضاء، ليتم الاطلاع عليها من طرف الإدارة أو أشخاص مخولين آخرين، وذلك بإذن من القاضي المختص من عدمه. بعد تخزينها تظهر المعلومات في الملفات "Log" و"تتبع كل نشاط على الشبكة بأدق التفاصيل، والذي يسمح بتحديد الوصف الاستهلاكي، وإهتمامات مستخدم الانترنت"[1]. فهي مفيدة جدا لتحديد الأشخاص الذين أجرو مكالمة هاتفية من مكان ما أو اتصلوا بشخص، أو أولئك الذين زاروا موقعا غير قانوني أو نشروا محتوى مضر على الإنترنت. تبرز الترسانة القانونية الجزائرية في هذا المجال من خلال طابعها التطفلي (2)، في حين أن الأحداث الأخيرة المتعلقة بكشف برامج التجسس الرقمي في جميع على المستوى العالمي أثار النقاش حول مدى توافق هذه التدابير مع قواعد حماية حقوق وحريات الأفراد(3).

1- رفع التستر أمام الالتزام بحفظ وتعريف البيانات التقنية.

يشير رفع التستر إلى الى الحالات التي ينص فيها القانون على أنه ولاستكمال التزام متعاملي الشبكات والوسطاء التقنيين للاحتفاظ بعدد من البيانات المتعلقة بمستخدمي خدمات الانترنت، يلتزم هؤلاء أيضا بتسليمها إلى السلطات المختصة لتسهيل التعرف على مرتكبي أعمال الاجرام الالكتروني. وفي هذا السياق أدخلت العديد من الدول استثناءات على مبدأ حذف أو تغفيل البيانات للسماح في ظروف معينة تبرير الاحتفاظ ببيانات الاتصال. وهذا يعني أن المتعاملين مع الجمهور مثل المقاهي والمطاعم والفنادق والمطارات أو أي هيئة أخرى والتي توفر الوصول إلى شبكة الإنترنت بمقابل أو بغير مقابل، تمسها هذه الأحكام، وبالتالي في كل هذه الأماكن كل اتصال بالشبكة يكون موضوع تسجيل

[1] A. Lucas, J. Devèze, J. Frayssinet, « Droit de l’informatique et de l’internet » PUF, Paris, 2001, p. 16.

ويتم الاحتفاظ بالبيانات لفترة معينة من الزمن. وفي وقت لاحق يصل المحققون إلى بيانات الاتصال بطريقتين، وفقا للطبيعة الإدارية أو القضائية للتحقيق. يجب عموما أن تتم الموافقة على تسليم البيانات بإذن من الجهة القضائية المختصة، على الرغم من أنه في بعض الأحيان ثمة استثناءات تسمح للإدارة أن تتدخل دون الاذن القضائي في التحقيقات المتعلقة بالجرائم الخطيرة مثل الإرهاب.

في أوروبا جاء التوجيه 58/2002 / EC الصادر في 15 مارس 2006 المتعلق بالاحتفاظ ببيانات الاتصال، والذي اعتمد نظرا للفوارق التشريعية التي كانت موجودة بين دول الاتحاد الأوروبي، ونص على مبدأ أن "البيانات (بيانات المرور والموقع) يجب أن تحذف أو أن يتم تغفيلها عندما لا تكون ضرورية لنقل الاتصال، باستثناء البيانات اللازمة لإعداد فواتير ومدفوعات الترابط "[1]. بالموازاة مع يتضمن النص في المادة 5 منه على أن الدول الأعضاء يمكن أن تضع قواعد تفرض الاحتفاظ ببيانات المرور لفترة محدودة عندما تشكل هذه القواعد "تدبيرا ضروريا، مناسبا ومتناسبا،ضمن المجتمع الديمقراطي، لحماية الأمن القومي – أي أمن الدولة – والدفاع والأمن العام، أو ردع والبحث والكشف ومتابعة الجرائم". ثم وبموافقة المستخدم، يمكن أيضا أن يتم تخزين بعض البيانات التي سيتم معالجتها لأغراض تجارية أو لتوفير خدمات ذات القيمة المضافة. وأخيرا فإن المادة 15 من التوجيه تسرد الشروط التي يمكن للدول الأعضاء أن تضع بموجبها استثناءات على مبدأ الحذف أو التغفيل. التدابير المتخذة يجب أن تكون ضرورية ومناسبة ومتناسبة، لأسباب محددة من النظام العام، أي لحماية الأمن القومي (أمن الدولة) والدفاع والأمن العام، أو لضمان ردع والبحث والكشف

---

[1] ويتعلق التزام الاحتفاظ بالبيانات لأغراض إعداد الفواتير بخدمات من قبيل التلفزيون المباشر، واقتراح تخزين البيانات عن بعد (الحوسبة السحابية)، وتوفير برامج متنوعة، وخدمات أخرى. التي تقدمها شركات الاتصالات الإلكترونية لزملائها.

ومتابعو الجرائم أو الاستخدام غير المشروع لأنظمة الاتصال عبر النترنت. بالفعل اعتبر المشرع الاوروبي ولهذه الأساب، أنه بامكان الدول الأعضاء أن تحدد آجالا للاحتفاظ بالبيانات تتراوح من ستة أشهر إلى سنة واحدة.

ولكن في حكمها الصادر في 8 افريل 2014 عارضت محكمة العدل الأوروبية الفيش الآلي للاتصالات عبر الإنترنت عن طريق الغاء التوجيه 24/2006 / CE التي جاءت عدّل توجيه 2002[1]. وأكد القاضي الأوروبي في حكمه على أنه "على الرغم من أن التوجيه المتعلق بالاحتفاظ بالبيانات لا يسمح بالاحتفاظ بفحوى الاتصالات والمعلومات التي تم تصفحها عبر الانترنت، لا تستبعد المحكمة أن المحافظة على البيانات ذات الصلة قد تؤثر على استخدام المشتركين أو المستخدمين المسجلين لوسائل الاتصال التي يستهدفها التوجيه، وبالنتيجة على ممارسة هؤلاء لحريتهم في التعبير، التي تكفلها المادة 11 من ميثاق الحقوق الأساسية للاتحاد الأوروبي ".

لا يوجد في الوقت الحاضر في الولايات المتحدة الأمريكية، أي تشريع يلزم مقدمي خدمات الإنترنت ومتعاملي الهاتف النقّال الاحتفاظ بالبيانات التقنية لمشتركيهم. بشكل عام يقوم مقدمو خدمات الإنترنت بحذف البيانات بمجرد نهاية صلاحيتها، أي الوقت اللازم لإعداد الفواتير و لحاجات تجارية أخرى.

إن الاتجاه الحالي بشكل عام هو اعتماد تدابير تقييدية من أجل مواجهة فعّالة لخطر الإرهاب و الاجرام الالكتروني. وهكذا وبعد بريطانيا التي تبنت "قانون الاحتفاظ بالبيانات وسلطات التحقيق" في 2014، بدورها أستراليا تبنت

---

[1] CJUE, gde ch., 8 avr. 2014, arrêt dans les affaires jointes C-293/12 et C-594/12 Digital Rights Ireland et Seitlingere.a., préc. V. Emmanuel Derieux, « Lutte antiterrorisme et protection des données personnelles: Durée de conservation des données de communication Invalidité de la dir. n° 2006/24/CE », RLDI 2014, n° 104, mai 2014.

"للاتصالات (الاعتراض والوصول) تعديل (الاحتفاظ بالبيانات) بيل" في 2015. في حين أن القانون البريطاني يلزم مقدمي خدمة الانترنت بالاحتفاظ ببيانات الاتصال لمدة سنة واحدة، ذهب القانون الأسترالي إلى أبعد من ذلك بتحديده لفترة سنتين. تم انتقاد القانونين من طرف المدافعين عن الحقوق الأساسية للأفراد. في اشارة الى القانون البريطاني اعتبر إدوارد سنودن على سبيل المثال، أنه يشبه كثيرا مثل "قانون حماية أمريكا" لسنة 2007 والذي أذن بإنشاء برنامج المراقبة PRISM في الولايات المتحدة الأمريكية[1]. وبالإضافة إلى ذلك فإن "قانون مكافحة الإرهاب والأمن" المعتمد في 12 فيفري 2015 يوسّع نطاق تدابير الاحتفاظ بالنص على جمع بيانات أخرى، مثل عناوين بروتوكول الانترنت IP.

2- الطابع الاباحي للنظام الجزائري.

إن التدابير التي اتخذتها الجزائر في مجال الحفظ (أ) وارسال (ب) البيانات من طرف متعاملي الشبكات ومقدمي خدمات الإنترنت تجعل من بلدنا من بين الأكثر تساهلا من حيث الصلاحيات الممنوحة للسلطات الإدارية.

أ- قواعد فرض التزام الحفظ.

إن الإلغاء الأخير للتوجيه الأوروبي CE/24/2006، والذي استوحت منه الدول الأوروبية قواعد حفظ البيانات التقنية ينبغي أن تؤثر على النظم الوطنية. ولكن حتى الآن ليس هو الحال في النظام الفرنسي الذي اقتبس عنه المشرع الجزائري القواعد الأكثر تساهلا من حيث الاحتفاظ بالبيانات. وفي حين أن المشرع الأوروبي يتجه نحو حماية حرية الاتصال من خلال معارضة المراقبة الشاملة للإنترنت[2]، فإن النظام الفرنسي والجزائري يسيران في الاتجاه المعاكس.

---

[1] أنظر:-http://www.theguardian.com/world/2014/jul/13/edward-snowden-condemns-britain-emergency-surveillance-billnsa

[2] "أستُخدم مصطلح «المراقبة الشاملة» من قبل البروفيسور أرمان ماتلار، وهو أستاذ في علوم الاتصال والإعلام بجامعة باريس، في كتابه «المراقبة الشاملة.. أصل النظام الأمني»، الذي

بشكل عام يلتزم مقدمو خدمات الإنترنت بحفظ البيانات التقنية التي تسمح بالتعرف على مستعملي الخدمة. تحدد مدة حفظ البيانات المذكورة في المادة 11 من قانون 04/09 بسنة واحدة ابتداءا من تاريخ التسجيل.

ب- القواعد المنظمة للوصول الإداري إلى بيانات الاتصال.

شهد حق الوصول إلى بيانات الاتصال تحولات عميقة لم تكن محل نقاش عام ولا محل اهتمام الرأي العام، حيث تم تكريس هذا الحق لفائدة السلطات العمومية، وبصفة خاصة السلطة ومصالح الأمن، ومؤخرا الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنونلوجيات الاعلام والاتصال ومكافحتها[1]. النتيجة اليوم هو أننا أصبحنا أمام نظام معقد، حيث تنص قوانين مختلفة على أساليب تدخل السلطات العمومية.

كل ما سبق يقودنا إلى الاستنتاج بأن الوضع الراهن للتشريع بشأن حماية الحريات العامة للأفراد - بما في ذلك حرية التعبير والاتصال - يعاني من نقائص كبيرة. وقد ظهرت هناك فجوة بين التطورات التكنولوجية في السنوات الأخيرة والتشريعات الرامية إلى ضمان احترام حقوق الأشخاص. ومن بين الثغرات الموجودة تدابير التصفية المختلفة التي تشير بصفة خاصة إلى عدم

صدر بدعم من وزارة الثقافة الفرنسية. وقد صدرت الطبعة الأولى المترجمة من الكتاب في عام 2013، عن شركة المطبوعات للتوزيع والنشر. واستخدم الكاتب مصطلح المراقبة الشاملة، لتوصيف مجموعة الخيارات الأمنية القائمة على المراقبة والتتبع والرصد، التي اتخذها عدد من البلدان الغربية بعد أحداث 11 سبتمبر 2011، لتأمين أراضيها من الاعتداءات الإرهابية". «المراقبة الشاملة» لم تمنـــع الإرهاب في الغرب، جريدة الامارات اليوم، 23 أوت 2017.

[1] المرسوم الرئاسي رقم 15-261 مؤرّخ في 8 أكتوبر سنة 2015 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وجود إشراف قضائي على اجراءات المراقبة والذي يكون كافيا لضمان احترام حريات الأفراد في الواقع الرقمي.

إن الرصد الالكتروني و تكنولوجيات المراقبة الرقمية تشكل مخاطر أخرى لاسيما من خلال التعقب الرقمي للأشخاص.

3- بين التعقب والمراقبة الرقمية.

إنه لا من الطبيعي أن نفكر بأن الطريقة غير المباشرة لردع الجرائم الإلكترونية والجرائم المتصلة بتكنولوجيا المعلومات والاتصالات ستكون بالحد من عدم تستر المستخدمين، وذلك أنه تحت غطاء التستر، يتصرف الأفراد تصرفات لامسؤولة ويمكن لهم ارتكاب الجرائم، لافتراضهم أن أفعالهم تبقى غير قابلة للكشف. بطبيعة الحال إذا تنقل المستخدمون في الفضاء الرقمي باستعمال هويتهم الحقيقية أو بالكشف عن بيانات تعريفهم، كنا أمام نسبة منخفضة في ارتكاب الجرائم الإلكترونية. لكن تعميم شرط تحديد الهوية من شأنه من جهة أن يشكل تحديا تقنيا لما يتطلبه من جمع وتخزين ونقل البيانات لتعريف المستخدمين على شبكة الإنترنت والذي يواجه عقبات تقنية تتميز بها الانترنت، ويشكل أيضا مساس بمبدأ التستر- أساس عمل شبكة الإنترنت - والذي يشكل بالضرورة وبحكم طبيعته من جهة أخرى انتهاكا للحق في حرمة الحياة الخاصة للأشخاص(أ).

لذلك فإن حالات رفع التستر على الانترنت يجب أن تكون متوازنة مع حرية كل مستخدم في الحفاظ على سرية بياناته التعريفية. رغم أنه وبعد الكشف عن برامج المراقبة الشاملة للبيانات المتبعة في الولايات المتحدة الأمريكية وبعض الحكومات الأوروبية أضرّت بشرعية وحق وصول السلطات العمومية إلى بيانات الاتصال (ب).

أ- نقاط التعارض مع مبدأ سرية البيانات.

إن التفرقة بين البيانات المتعلقة بالاتصال ومحتوى هذا الأخير تبقى دقيقة نظرا للتداخل القوي في اطار شبكة الإنترنت بين البيانات اللازمة لإقامة الاتصال" وتلك المتعلقة بمحتوى الاتصال[1]. في نهاية المطاف فإن الجدل المتعلق بحفظ والابلاغ بالبيانات يشكل تعارضا بين فكرتين أساسيتين: من جهة تتمثل الأولى في حد أدنى من الحفظ لأسباب تتعلق بالتكاليف والصعوبات التقنية لتطبيقه، وحماية للحياة الخاصة للأفراد(حماية البيانات التعريفية) أو فلسفة شخصية (تصور الإنترنت بوصفها فضاء للحرية)، ومن جهة أخرى تتمثل الفكرة الثانية في الحفظ على أعلى مستوى، لأسباب الأمن ومكافحة الجريمة الإلكترونية، والحماية الفعالة لحقوق الملكية الفكرية أو للحق في الصورة، الخ.

وأخيرا وحتى يعتبر شرعيا يجب أن يكون نظام المراقبة قد أذن به القانون. على هذا النحو اعتبرت المحكمة الأوروبية لحقوق الانسان في قضية كوبلاند ضد بريطانيا أن استخدام أجهزة تنصت سرية وجمع وتخزين المعلومات المتصلة باستخدام المدعية لهاتفها، وبريدها الإلكتروني والإنترنت، لم يتم "وفقا للقانون "، باعتبار أنه لم يكن هناك أي تشريع داخلي ينظم هذه المراقبة وقت الوقائع.

ب- خطر المراقبة الشاملة للآثار الرقمية من طرف السلطة العامة.

إن شبكات الاعتراض العالمية للبيانات ليست وليدة القرن الحادي والعشرين. كان الأمر يتعلق في السابق باعتراض سلكي أو عن طريق الأقمار الصناعية ويهدف أساسا لرصد القدرات النووية للدول (الاتحاد السوفييتي بصفة خاصة)،

---

[1] Forum des droits sur l'Internet, Rec. aux pouvoirs publics: « Conservation des données relatives à une communication électronique », 18 déc. 2001.

واليوم أصبح الإرهاب من يحفز اعتراض الاتصالات الإلكترونية عبر الشبكة الرقمية[1]. وبالمقابل فإن مخاوف المعارضين تطورت بشأن هذه الاختراقات – في حين أنه سابقا كان التخوف من الاستخدامات المحتملة للمعلومات التي تم جمعها لغرض التجسس الاقتصادي[2]، حاليا تظهر أساسا القضايا المتعلقة بالحريات الأساسية للأشخاص والتي ينصب عليها النقاش.

لم يتطرق المشرع الجزائري إلى تحديد ما المقصود بمراقبة الاتصالات الإلكترونية وإنما إكتفى بتحديد مفهوم الاتصالات الإلكترونية[3]. ونشير إلى أن المشرع الجزائري وإن أباح مراقبة الاتصالات الإلكترونية في نص المادة 65 مكرر 5 رغم إستعماله مصطلح الإعتراض بدل المراقبة إلا أنه يحمل نفس المعنى. في خمس(05) جرائم فقط محددة على سبيل الحصر، إلا أنه رجع في نص المادة (03) من القانون 09 / 04 وجعلها مطلقة تشمل كافة الجرائم ولكن في حالات محددة وهي: في حالة حماية النظام العام، أو لمستلزمات التحريات، أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون لإجراءات الجزائية، وكذا القانون 09 / 04 هذا مع عدم المساس بجملة من الضمانات من أهمها أن تكون تحت إشراف جهات قضائية.

---

[1] S-Y. Laurent, « Liberté et sécurité dans un monde anomique de données », CNCIS, 22e rapport d'activités, 2013-2014, p.16, adresse: http://convention-s.fr/wp-content/uploads/2015/04/Libert%C3%A9-et s%C3%A9curit%C3%A9-dansun-monde-anomique-de-donn%C3%A9es.pdf.

[2] F. Lafouasse, « L'espionnage dans le droit international », Paris, Nouveau monde éditions, « Le Grand jeu », 2012, p491.

[3] المادة 02 فقرة(و)من القانون 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: " أي تراسل أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية ".

كما جاء في المادة 04 من القانون 09 / 04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، أنه يجوز القيام بعمليات المراقبة المنصوص عليها في المادة 03 من ذات القانون في الحالات التالية:

1 – الوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو التخريب، أو الجرائم الماسة بأمن الدولة: يفهم هنا أن المشرع أجاز المراقبة المسبقة للإتصالات الإلكترونية، أي قبل إرتكاب الجريمة فالوقاية هنا تسبق عملية البدئ في التنفيذ وتسبق حتى عملية التحضير للجريمة، وعليه فبمجرد توافرر شكوك ولو بسيطة أن هناك إحتمال قيام شخص أو مجموعة من الأشخاص بالتحضير لإحدى الجرائم سالفة الذكر، يجعل مراقبة إتصالاتهم الإلكترونية من قبل السلطة المختصة فعلا مشروعا.

نشير هنا أن هذا الفرض يعتبر إعتداء صارخ على حقوق الأشخاص في سرية إتصالاتهم، لأنه بمجرد توافر شكوك ولو بسيطة عن إحتمال تورط أشخاص في التحضير لإحدى الجرائم السابقة يجعل من إعتداء السلطات على حقهم في سرية مراسلاتهم المقرر لهم بموجب الدستور و عدد من المواثيق الدولية عملا مشروعا، خاصة مع ما تتسم به هذه الجرائم من خصائص كونها صعبة الإكتشاف، وحتى إن إكتشفت فهي صعبة الإثبات، وإن أثبتت يبقى مشكل الإختصاص القضائي في أحيان كثيرة عائقا أمام توقيع العقاب على مرتكبيها، فكيف يمكن أن يتحقق هنا عنصر الشك في إحتمال إرتكاب هذه الجرائم، إذا كانت مع وقوعها وتحققها صعبة الإكتشاف؟

ومع هذا يمكننا القول أنه إجراء وقائي أقره المشرع للوقاية من جرائم محددة على سبيل الحصر ألا وهي جرائم الإرهاب، التخريب، أو الجرائم الماسة بأمن الدولة، لما تتسم به من خطورة بالغة على الدولة، كما يمكن أن يصل مداها إلى المجتمع الدولي ككل.

2–في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو الدفاع الوطني، أو مؤسسات الدولة، أو الاقتصاد الوطني: نشير إلى أن المشرع أجاز المراقبة المسبقة للإتصالات الإلكترونية حماية لمجموعة من المصالح والهيئات" النظام العام، الدفاع الوطني، مؤسسات الدولة، الإقتصاد الوطني."

وعليه فهذا الإجراء هو الآخر إجراء وقائي، لأنه بمجرد توافر معلومات عن إحتمال إعتداء على منظومة معلوماتية تمس بالمصالح السابقة، يجعل من إجراء المراقبة الرقمية فعلا مشروعا ويستوي أن تتوفر هذه المعلومات من قبل السلطات ذاتها، أو من قبل البلاغات والشكاوى التي ترد إلى السلطات من قبل المواطنين، المهم أن تنبئ هذه المعلومات عن إحتمال إعتداء على هذه المصالح والهيئات سالفة الذكر، و نشير إلى أن المشرع لم يكتفي هنا بمجرد الشك و إنما إشترط أن تتوفر معلومات عن إحتمال إعتداء على منظومة معلوماتية تمس بهذه الهيئات والمصالح.

فالمشرع أجاز هذا الإجراء ليس للوقاية من جرائم محددة على سبيل الحصر كما جاء في الفقرة 01 من هذه المادة وإن كان يشملها، لأن في إرتكاب أي جريمة من تلك الجرائم المذكورة على سبيل الحصر فيه مساس بهذه المصالح والهيئات.

ويعتبر هذا النوع من الجرائم من أخطر الجرائم على الإطلاق، خاصة مع السياسة التي إعتمدت عليها البلاد في عصرنة كافة القطاعات، وذلك بالاعتماد المتزايد على أنظمة المعلومات فحساسية هذه القطاعات كالدفاع الوطني تستوجب المراقبة المسبقة، لما لها من تأثير على كيان الدولة ككل في حالة المساس بها.

3– لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية:

يعتبر هذا الإجراء ليس وقائيا فحسب وإنما هو إجراء قضائي، لأنه يتم في مرحلة البحث عن الدليل، وليس في مرحلة ما قبل الشروع في الجريمة كما جاء سابقا، ونشير إلى أن اللجوء إلى مراقبة الاتصالات الإلكترونية هنا لا ينحصر على تلك الجرائم المحددة سابقا، و إ نما يتعداها إلى كافة جرائم القانون العام، بشرط أن تكون هناك صعوبة في الحصول على نتيجة تهم الأبحاث دون اللجوء إلى المراقبة الإلكترونية.

4- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة : يدخل هذا في إطار التعاون الدولي للحد من الجرائم العابرة للحدود كما هو الشأن بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والإتصال، فمثلا كما لو طلبت دولة أخرى من الجزائر بمراقبة أو السماح لها بمراقبة الاتصالات الإلكترونية لأشخاص مقيمين في الجزائر، يحتمل إشتراكهم في عمل إجرامي بالخارج مس بالدولة الطالبة، هنا يجوز للسلطات الجزائرية مراقبة هذه الاتصالات، أو السماح لها بمراقبة إتصالات هؤلاء الأشخاص، وهذا طبعا دون المساس بالإتفاقيات الدولية ومبدأ المعاملة بالمثل[1].

إلا أن الجانب الأكثر مدعاة إلى القلق هو تغير المفاهيم في اضفاء الشرعية ليس فقط على الاعتراض لأغراض جزائية، ولكن أيضا لأغرض وقائية ومخابراتية. وهو نتيجة مباشرة للتطرف السائد المؤدي إلى تعميم النظريات المتعلقة بحالة الطوارئ بعد الهجمات الإرهابية المختلفة التي حدثت منذ هجمات 2001[2] وبمجرد أن نقبل بهذا، فإن الخطوة التالية هي أن نقبل ليس فقط

---

[1] جبار فطيمة، مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، العدد الثالث ديسمبر 2016، ص 17.

[2] Eric Sadin, « Surveillance globale. Enquête sur les nouvelles formes de contrôle », Paris, Climats, 2009 ; M. Foessel, « État de vigilance. Critique de la banalité sécuritaire », Paris, éd. Les bords de l’eau, 2010.

بممارسات لمراقبة مؤقتة و محددة (*targeted surveillance*)، ولكن أيضا تلك العامة والدائمة (*dragnet surveillance*)[1]. إن المراقبة المحددة التي تهدف لحماية الدول من التهديدات ضد أمنها القومي لم تعد تثير الاستغراب، واستخدمت بشكل منهجي عبر التاريخ. ولكن فضائح وكالة الامن القومي الأمريكية NSA قد أثارت مخاوف جدية حول الجمع والتحليل الشامل لبيانات المواطنين الذين لا يشتبه في صلتهم بالإرهاب أو بأشكال أخرى من الاجرام.

وتبعا لهذه المقاربة فإن الآثار الرقمية الواجب اتباعها لم تعد تقتصر على الأشخاص المشتبه فيهم وذلك لأن المراقبة الشاملة – التي تشمل معلومات جميع السكان – هي الوحيدة التي تتمكن من التقاط إشارات معزولة تؤدي إلى المجرمين الحقيقيين[2]. على سبيل المثال وكما ورد في تقرير لجنة الشؤون القانونية وحقوق الإنسان التابعة لمجلس أوروبا، فإن وكالة الأمن القومي الأمريكية NSA بتجسسها على اتصالات الأشخاص ركّزت وبصفة خاصة على مستخدمي أنظمة التشفير والتستر لإخفاء تدفق البيانات. مجرد البحث في الانترنت على برمجيات التشفير وتعزيز أمن البيانات أدى بالوكالة الأمريكية للأمن القومي إلى تحديد ومراقبة عنوان برتوكول الانترنت IP الخاص بصاحب البحث، بغض النظر عن البلد الذي كان فيه.

إن حقيقة وجود الأنظمة الكبرى التي وضعتها أجهزة الاستخبارات الأمريكية وبعض شركاءها الأعضاء في مجلس أوروبا تم تأكيدها من طرف العضو السابق في وكالة الأمن القومي الأمريكي إدوارد سنودن Edward Snowden منذ

---

[1] J. Appelbaum, Intervention au Cons. E., 28 janv. 2014.

[2] Sur la notion de surveillance de masse, v. M. Cusson, « La surveillance et la contre-surveillance », in: M. Cusson, F. Lemieux, B. Dupont, « Traité de sécurité intérieure », Lausanne, Presses polytechniques et universitaires romandes, 2008, p. 429-436.

جوان 2013. وكان هدفهم هو جمع وحفظ وتحليل البيانات المتعلقة بالاتصالات الالكترونية على نطاق واسع بما في ذلك بيانات حركة الانترنت، بل أيضا ذات المحتوى وبيانات الموقع و غيرها من البيانات الوصفية[1].

وفي الوقت الذي تظهر فيه المحكمة الأوروبية لحقوق الإنسان توجها واقعيا في مواجهة الإرهاب، في اجتهاداتها[2] وكذا في التصريحات العلنية لرئيسها[3]، إلا أنها الحامية لقيم المجتمع الديمقراطي والحريات والحقوق الأساسية التي تكفلها الاتفاقية الأوروبية لحقوق الإنسان. وفي هذا الصدد تُذكر المحكمة في قرارها Szab□ و Vissy بأن مكافحة الإرهاب لا تكفي لتبرير جميع القيود المفروضة على الحقوق والحريات التي تفرضها الدول التابعة للاتحاد في تشريعاتها الداخلية وأن سلطات المراقبة السرّية للأفراد غير مقبولة بناءا على الاتفاقية الأوروبية إلا في حالة ضرورة الحفاظ على المؤسسات الديمقراطية[4].

ثانيا: المراقبة من خلال التعرف على الأشخاص.

تضع الدول أنظمة للهوية الرقمية المسلمة من طرف مرفق تابع للسلطة العامة من جهة (1) كما أن مقدمي الخدمة يبحثون دائما عن طرق جديدة للتعرف

---

[1] أنظر:

Conseil de l'Europe, « Les opérations de surveillance massive », rapport de la Commission des questions juridiques et des droits de l'homme, doc. n° 13734, 18 mars 2015, p. 2, adresse:
http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21583&lang=fr.

[2] V. en dernier lieu CEDH, 20 oct. 2015, n° 5201/11, Sher et a. c/ Royaume-Uni: Gaz. Pal. 28 nov. 2015, p. 20, n° 248s5, obs. J. Andriantsimbazovina.

[3] G. Raimondi, « Face au terrorisme, la CEDH doit être réaliste »: Le Monde 15 janv. 2015.

[4] CEDH,Szabo et Vissy c. Hongrie, 12 janvier 2016.

على الأشخاص في اطار أنشطتهم عن طريق تعقب البيانات التي يقدمونها أو التي يتم جمعها عنهم (2).

1- الأنظمة الحكومية في التعريف الالكتروني.

كما ذكرنا في المباحث السابقة كل مستخدم للانترنت يبني وجود افتراضي متفاوت التطور. بمجرد أن يتصل، تنشأ علاقة بالضرورة بينه وبين مستخدمين آخرين، والذي يعطي لهذا الوجود طابع قانوني: سواء كان ذلك في اطار علاقات تجارية أو إدارية، في شكل من أشكال العقود، أو من خلال عمليات الدفع الالكتروني. في هذا السياق من الضروري أن يتم التعرف على الأشخاص رغم المبدأ الأساسي في عمل الإنترنت والذي يضمن لهم درجة معينة من التستر(أ).

أبعد من ذلك فإن انشاء الحكومة لنظام الهويات السيادية الرقمية يسمح بادارة مشاركة المواطنين في المعاملات عبر الإنترنت، ووصولهم إلى البيانات والمحتويات (ب).

أ- مبدأ التعريف بالهوية على الانترنت واستخدام اسم مستعار.

إن منح الهوية الرقمية في اطار أساليب التعريف الرقمي يكون بإصدار شهادة إلكترونية صادرة عن جهة موثوق فيها. وفي هذا الاطار يختلف الإجراء المطبق حسب درجة التجريد. يتم التسجيل مباشرة وفقط عبر الإنترنت. في هذه الحالة، يكون التأكد من هوية المستخدم المعلنة ليست كاملة ويتعلق الأمر بتحديد للهوية يكفل الحد الأدنى من الأمن. ويمكن أيضا أن يتم التسجيل على الانترنت بارسال عن طريق البريد لوثائق تثبت هوية الأشخاص المعنوية و / أو الطبيعية التي صرّح بها صاحب الشهادة.

وبالتالي تشكل الهوية الرقمية عنصر أساسي في استخدام التكنولوجيا الرقمية في اطار العلاقات المدنية والتجارية والإدارية. ولها تطبيقات متعددة في الواقع:

حيث تعتبر الهوية الرقمية شرطا للأمن القانوني للعلاقات غير الملموسة ذات الطابع التجاري أو الإداري أو مجرد مراسلات الكترونية خاصة. لذا فإن الحق في التستر لا يمكن أن يطبق هنا، حيث هناك خطر في إلغاء المعاملات القانونية المبرمة إلكترونيا أو في قيام الأشخاص بارتكاب أعمال إجرامية باستخدام البيانات والشبكات عن طريق الاحتيال – مثل نشر المحتوى غير المشروع، وانتحال الهوية، والتصيد، وبيع السلع المقلدة، الخ.

ب- تجريد النظم الحكومية في تحديد الهوية أمام مخاطر جمع البيانات البيومترية.

إن القواعد الأوروبية الجديدة والتي اقتبسها المشرع الجزائري تشجع إقامة أنظمة الهوية الرقمية، بغض النظر عن ما إذا كانت مادية ("*tokens*" أو جهاز رموز الأمان، يقوم بعرض رموز رقمية عند الضغط عليه، وهذه الرموز عبارة عن مجموعة من المتغيرات كعامل الوقت حال الضغط على الزر واسم المستخدم واسمه الحقيقي وغيرها. وتعتبر وسيلة آمنة حيث تضيف داعماً آخر بالاضافة لاسم المستخدم وكلمة المرور) أو غير الملموسة (الشهادات الالكترونية). إن الهدف إذن من ذلك هو إنشاء نظام يكون فيه كل شخص قادر على تحديد هويته الحقيقية، عبر وسيلة إلكترونية ويمكن التحقق منها من قبل طرف ثالث أو خدمة الانترنت، من خلال استخدام بطاقة تعريف مجردة على سبيل المثال. اختيارية أو اجبارية تسمح هذه الوثيقة للأفراد من تحديد هويتهم والتوقيع بشكل عالمي وآمن، شريطة الالتزام باحترم الحريات الأساسية للأفراد في العالم الرقمي.

على هذا النحو مجموعة من الوثائق مثل جواز السفر، رخصة القيادة أو بطاقة الهوية أصبحت موضوعا لهذه القواعد الجديدة. حيث يتم وضع شريحة بداخلها من تحتوي على شهادات التعريف والتوقيع. في الجزائر مكّن القانون رقم

14/03 الصادر في 24 فيفري 2014 المتعلق بسندات وثائق السفر من تبني نظام جواز السفر البيومتري.

2- تعقب الأشخاص من خلال مختلف البيانات الرقمية.

يمكن للهوية الرقمية في الحقيقة أن تأخذ أشكال عدة في عالم الانترنت[1]. حيث يتعين التمييز بين الهوية في شكلها الرقمي التي تقع تحت السلطة السيادية للدولة، وتشمل البيانات الحقيقية (الاسم، العنوان، تاريخ ومكان الميلاد...) والبيانات الرقمية التي يمنحها مقدمو الخدمة أو يتم اختيارها من طرف مستخدمي الإنترنت أنفسهم ومقبولة من طرف مقدمي الخدمة للوصول إلى خدماتهم. ناقشنا في المباحث السابقة أن كل مرور عبر الإنترنت يترك آثار الرقمية التي يمكن أن تكون مقصودة أو غير مقصودة من طرف المستخدم. ويمكن أن تتراوح من عنوان البريد الإلكتروني البسيط، إلى اسم الدخول و كلمة السر، إلى عنوان بروتوكول الانترنت IP، واسم النطاق أو الاسم المستعار[2]، أو حتى توقيع خطي ممسوح ضوئيا.

عمليا يتم التعقب عبر مجموعة من الأدوات المختلفة، وتشكل شبكة الإنترنت الوجه الأوسع له والأكثر تنوعا. تشارك الكوكيز في هذا العالم بالحفاظ على آثار المواقع التي تم زيارتها لتعريف المستخدمين وربما حفظ ملفاتهم الشخصية. ولكن يتم التعقب أيضا من خلال الاتصالات الهاتفية. من اللحظة التي يلتزم فيها متعاملو الهاتف النقال بحفظ وتسليم بيانات الموقع الجغرافي للشرطة، حيث تكون قادرة على التعقب التلقائي لحركة الأشخاص المعنيين على الخريطة.

---

[1] G. Desgens-Pasanau, E. Freyssinet, « L'identité à l'ère numérique », Dalloz-Sirey, Coll. Presaje, 2009.

[2] Olivier Itéanu, « L'identité numérique en question », Paris, Eyrolles, 2008, v. spéc. p.5 à 22.

أساليب التحقيق الجديدة.

أمام التحولات التي يشهدها الاجرام، فإن المراقبة عن بعد تأتي كإضافة إلى الإمكانيات المهمة أيضا و المتمثلة في كاميرات المراقبة، تحديد الموقع الجغرافي أو اعتراض البيانات (أولا).

هذه الوسائل الرقمية المختلفة تسمح ليس فقط بالبحث عن مرتكبي الجرائم، ولكن أيضا في استباق التهديدات من خلال التحليلات التنبؤية المتطورة (ثانيا).

أولا: الوسائل الجديدة في ظبط بيانات الشبكة.

إن النظام الذي يهدف إلى تأطير الاعتراض الشرعي للمراسلات (1) – القضائي والإداري – الذي يهدف من جهة إلى تقديم أدلة في اطار التحقيق، ومن جهة أخرى لتحديد المخاطر المحتملة المتصلة بالمجرمين والارهابيين يجب أن يوازن بين متطلبات المراقبة والنظام العام مع مقتضيات احترام الحريات العامة. بالاضافة إلى إجراء الاعتراض هناك إمكانية القيام بعمليات التفتيش الالكتروني في سياق الجرائم الإلكترونية(2). وبعد ذلك سنتطرق إلى الشروط اللازمة لاجراء شكل خاص من أشكال التفتيش، والتي تتمثل في التقاط البيانات الرقمية عن بعد، والتي تُعد بيانات تحديد الموقع الجغرافي على وجه الخصوص جزءا منها (3) ثم نتعرض في الأخير إلى تقنية حديثة تتمثل في التسرب الالكتروني(4).

1- الاعتراض الشرعي لمحتوى المراسلات.

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرّر في المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور.

لم يسمح المشرع بهذا الاجراء إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته، وهذا ما قررته المادة 04 من القانون 04/09 التي جاء فيها أنه: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة "[1].

شهد تطبيق نظم اعتراض الاتصالات السلكية واللاسلكية ثم الاتصالات الإلكترونية في الدول الغربية مرحلتين مختلفتين: الأولى كانت تهدف إلى الحد من عدد الاعتراضات وتوفير ضمانات للحفاظ على سرية المراسلات، بإنشاء هيئات رقابة. وشملت العقدين الأخيرين من القرن العشرين. والمرحلة الثانية تدخل في إطار السياسة الأمنية التي تستخدم فيها المراقبة بالفيديو، البيومترية، الخ. في حين يستخدم الأشخاص العامة الاعتراض بشكل متزايد ومتكرر، فإن هيئات الرقابة لا تزال موجودة وتشكل إحدى معاقل المقاومة القليلة لايديولوجية الأمن التي تتجلى في نهاية القرن العشرين وبداية القرن الواحد والعشرين. –يشكل الاعتراض الالكتروني اليوم وسيلة فعالة لمكافحة الجرائم الالكترونية، ردا على التهديدات المفترضة عندما يتعلق الأمر بالاجرام و المحتملة في حالة الأعمال الإرهابية.

لا يهتم المحققون فقط بمحتوى المحادثات أو المراسلات، بل يبحثون أيضا عن بيانات متعلقة بمعلومات معينة: من كان على اتصال مع من، متى وأين. يمكن أن تكشف هذه المعلومات في مستوى ثاني (متعلق بظروف الاتصال) عن هيكل شبكة إجرامية أو إرهابية وحالة نشاطها، دون أن يضطر بالضرورة إلى معرفة ما يقال[2].

---

[1] د. أمحمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية: (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد في الجزائر العاصمة يوم 29 مارس 2017، ص 57.

[2] Département De Recherche Sur Les Menaces Criminelles Contemporaines, Actes du colloque « Ecoutes et interceptions légales des

بيانات الاتصال المختلفة التي تم جمعها من خلال عمليات التفتيش الالكتروني وتدابير التقاط البيانات، تسمح في بعض الأحيان بالحصول على مبرر لاعتراض المحتوى من أجل استباق تهديد مكتشف.

2- التفتيش الالكتروني.

قررت المادة 5 من القانون رقم 09/ 04، أنه يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى: منظومة معلوماتية أو جزء منها وكذلك المعطيات المعلوماتية المخزنة فيها ومنظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة- أ- من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وإذا تبين مسبقا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

وكمثال على المساعدة القضائية الدولية كإجراء جديد لتتبع مجرمي المعلوماتية، قضية توقيف مصالح الأمن الجزائرية لشاب جزائري ببلدية

---

télécommunications. Les nouveaux enjeux technologiques et financiers », Paris II, 5 oct. 2006, p. 5, adresse:
http://drmcc10ans.org/IMG/pdf/Actes_Senat.pdf.

بومرداس بعد تقديم المكتب الفدرالي الأمريكي للتحقيقات شكوى ضده مفادها أن هذا الشاب قد بعث برسالة إلكترونية لهذا المكتب مهددا فيها بوضع قنبلة في أحد أحياء مدينة جوانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبل انطلاق المباراة الكروية بين المنتخب الجزائري والأمريكي في بطولة كأس العالم.

والمشرع الجزائري في المادة الخامسة من القانون رقم 04/09 نص على التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وأن اختلف مضمونه عن التفتيش العادي بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة 45 من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

غير أن القانون رقم 09/ 04 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد، وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها.

ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها.

كما نص المشرع الجزائري، ودائما في نفس القانون 04/09 على إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 5، وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن برمجة الحاسوب لإجراء عمليات التفتيش على المنظومة المعلوماتية، وجمع

المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات[1].

وتنص المادة 19 من اتفاقية بودابست لمكافحة الجرائم المعلوماتية على أنه يجوز للدول الموقعة أن تأذن بعمليات تفتيش الكترونية " في منظومة معلوماتية أو جزء منها و بيانات الحاسوب المخزنة فيه...وفي دعائم تخزين البيانات " في حدود اختصاصها الإقليمي.

وفي مواجهة هذه الأسئلة العديدة يجب توفير ضمانات خاصة بالوصول إلى محتويات أجهزة الحاسوب واستغلالها للحد من نطاقه والإشراف على الإجراءات وضمان احترام حقوق الأشخاص الذين يتم تفتيشهم قدر الإمكان، فضلا عن ضمان أمن عملية استغلال البيانات التي تم جمعها. وعلى وجه الخصوص يبدو أن الضمانات الإجرائية التي تخضع لرقابة القاضي اللاحقة ضرورية لحماية الأشخاص في مواجهة التفتيش التعسفي.

3- التقاط البيانات الرقمية عن بعد.

التقاط البيانات الرقمية عن بعد صورة من صور التفتيش الالكتروني، حيث يتم البحث والتقاط البيانات عن بعد، من مكتب التحقيق إلى المنظومة التي ارتكبت فيها الجريمة. ونتيجة لذلك فهو في الواقع في منتصف الطريق بين التفتيش واعتراض البيانات. ويستخدم غالبا في مرحلة التحقيق القضائي. ويهدف إلى منح المحققين القدرة على استخدام الأجهزة التقنية لالتقاط البيانات آنيا وهي بيانات تكون مستخدمة أو قيد الانشاء قبل أن يتم حذفها أو تشفيرها. عمليا قد يتعلق الأمر بالاطلاع على ملفات مسجلة، وقراءة مفاتيح اللوحة، من خلال تفعيل الميكروفون أو الكاميرا، تشغيل قرص مضغوط في محرك الأقراص أو الرصد

---

[1] د. أمحمدي بوزينة أمنة، المرجع السابق ص 57.

الآني لعمليات البحث على الإنترنت أو لمناقشات في غرف الدردشة، الخ. تحقيقا لهذه الغاية، يستخدم الضباط برامج تجسس، مثل السكريبات، والتي يمكن تركيبها ماديا وكذلك عن بعد باستخدام برامج تجسس مثل « *keylogger* »[1].

4- التسرب الالكتروني.

نص المشرع الجزائري على التسرب التقليدي وفقا للإجراءات القانونية المعمول بها وهو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم، فالتسرب إذن هو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم جريمة، أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم، ويسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة بعض الجرائم، دون أن يكون مسؤولا جزائيا، وذلك بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية[2].

لم ينص المشرع الجزائري عن الحالات الخاصة للتسرب في الواقع الرقمي أو ما يسمى بالتسرب الالكتروني و الذي كرسه المشرع الفرنسي بموجب قانون رقم 297/2007 الصادر في 05 مارس 2007 المتعلق بمكافحة جرائم الاتجار بالبشر ودعارة الأطفال[3] وبموجب قوانين أخرى إلى غاية تبني قانون مكافحة الارهاب في 13 نوفمبر 2014 الذي وسّع من دائرة اللجوء إلى هذا الاجراء إلى

---

[1] وظيفته هو مراقبة وتسجيل ضغطات المفاتيح التي يقوم المستخدم بضغطها ويقوم بهذه العملية بسرية ودون علم او شعور المستخدم بذلك.

[2] د. أمحمدي بوزينة أمنة، المرجع السابق ص 57.

[3] art. 706-35-1 du CPPF

الجرائم المنظمة بما فيها الأعمال الارهابية وانتقل التسرب الالكتروني من مجال الردع إلى الوقاية من هذه الجرائم[1].

من أجل تنفيذ هذا النوع من التدابير، تم في فرنسا إنشاء دوريات الكترونية وهي مصالح تحقيق مكلفة بالمشاركة في التبادلات الإلكترونية – على منتديات المناقشة على سبيل المثال – تحت اسم مستعار؛ والدخول في اتصال "بهذه الطريقة مع الأشخاص المحتمل أن يكونوا قد ارتكبوا هذه الجرائم " ؛ فضلا عن "استخلاص أو الحصول أو الاحتفاظ من خلال هذا التدبير بالأدلة والبيانات المتعلقة بالأشخاص المشتبه فيهم ارتكاب تلك الجرائم".

ثانيا: نحو تطوير أساليب تنبؤية للتحقيق.

إن النتائج التي تم الحصول عليها من خلال الوسائل التنبؤية يمكن أن يؤدي إلى تصنيفات كاذبة أو تمييزية بين الأفراد ويمكن أن تمس بمبدأ قرينة البراءة فيما تعلق بالنطاق الجزائي. إنها المشكلة الرئيسية في التنميط التنبؤي الذي يهدف إلى استباق سلوك الأفراد، سواء في اطار عاداتهم كمستهلكين، أو من خلال التحقيقات الجنائية (1). يتم استخدام آلية الوقاية أيضا في اطار تقاطع أنواع مختلفة من البيانات – بما في ذلك سجل حجز المسافرين PNR – وهذه المرة لمنع ارتكاب الأعمال الإرهابية (2).

1– التنميط التنبؤي كنتيجة لاستخدام وسائل التعقب.

واحدة من الخصائص الرئيسية للبيانات التي يتم معالجتها كبيانات ضخمة Big Data هي أنها على عكس البيانات التقليدية التي تم جمعها في قواعد بيانات منظمة، يتم معالجتها آنيا من المنطقي، مما يتيح الاستفادة منها، من استغلال كميات كبيرة من البيانات عن طريق التغلب على القيود التقنية التي تجعل هذا

---

[1] 706-87-1 du CPPF

التبادل صعبا، إن لم يكن مستحيلا، عندما تأتي هذه البيانات من عدة مصادر أو يتم تنظيمها بطرق مختلفة. لذلك فإن نتائج معالجة وتحليل هذه البيانات تتميز ببعدها الأكثر وضوحا وديناميكية. وبالتالي فإن البيانات الضخمة Big Data لا تجلب فقط تغييرا كميا في أنها تضاعف بشكل كبير من حجم البيانات، ولكنها أيضا تشكل تحولا نوعيا بحيث لم تعد المعالجة تشمل بيانات عيّنة ومنظمة، ولكن تشمل بيانات غير متجانسة ومتناثرة، منظمة وغير منظمة[1].

في هذا الصدد جاءت هذه التكنولوجيا مواتية تماما لمعالجة الآثار الرقمية التي يتركها الأشخاص على الانترنت. وسيشكل التنميط الناتج خطوة إلى الأمام بالمقارنة مع التقنيات السابقة. لن يتعلق الأمر بمعرفة من هو المستخدم المعني في الوقت المعين، وما هي اهتماماته ومصالحه في الوقت الذي يترك آثاره.

سيكون الهدف الآن هو التنبؤ استنادا إلى نفس العناصر، بما سيفعله هذا المستخدم بعد ذلك، واستباق رغباته واحتياجاته، ومعرفة استخداماته وسلوكياته المستقبلية، إلخ. ولذلك يجب التمييز بين النشاط الذي يتمثل في تلبية احتياجات المستهلكين وذلك الذي يهدف إلى توقعها[2]. إن الرغبة في التوقع يتمثل في الحقيقة في إنشاء ملامح تنبؤية [3]، حيث يعتبر الفرد شيئا من جهة، مما قد يشكل خطر

---

[1] Sarra Soltani, « Big Data et le principe de finalité », RLDI, n° 97, oct. 2013.

[2] L. Marini, R. Perray, op.cit.

[3] G29 souligne l'existence de deux catégories des profils des utilisateurs qui peuvent être constituées à ce titre. En effet, il distingue « les profils prédictifs [qui] sont établis par déduction en observant le comportement individuel et collectif des utilisateurs dans le temps, notamment en suivant les pages visitées et les publicités qu'ils ont vues ou sur lesquelles ils ont cliqué » et « les profils explicites [qui]sont établis à partir des données à caractère personnel que les personnes concernées fournissent elles-mêmes à un service web, notamment par leur inscription. Ces deux méthodes

المساس بكرامته وبسلامته، ومن ناحية أخرى يمكن أن يكون أثر المساس بحرمة الحياة الخاصة أو الحق في حماية البيانات مدمرا لأنه يقوم على الاحتمالات والتنبؤات.

بيد أن نفس الاشكالية موجودة فيما يتعلق بالتنميط التنبئي الذي تستخدمه السلطات الأمنية بانتظام، ويتم دمجه على نحو متزايد في النظام الإجرائي، من أجل تحديد الأفراد الذين قد يخضعون للمراقبة أو لاهتمام خاص. ومن ثم فإن استخراج البيانات سيجعل من الممكن إنشاء "بروفايلات" أو ملفات شخصية عن طريق جمع البيانات الشخصية وضمها لبعضها البعض وتحليل هذه البيانات بالنظر إلى سلوكيات معينة تعتبر مشبوهة. ولكن في غياب ضمانات كافية، ليس مستبعدا أن اجراء تقاطع للبيانات يمكن أن يتم جزئيا على أساس التعميمات النمطية المتعلقة بالانتماء العرقي أو الديني أو بجنسية الأشخاص، خاصة في مجال مكافحة الإرهاب. وهكذا يتم البحث بطريقة واسعة، بغض النظر عن حالة معينة، وقد يؤدي إلى الاشتباه بأشخاص أبرياء مشبوهين بالاعتماد على "بروفايلات" أو ملفات شخصية خاطئة، في خرق لضمانات أساسية والمتمثلة في مبدأ الوجاهية وقرينة البراءة[1].

2- تبادل البيانات وترابطها: بيانات سجل حجز المسافرين PNR كمثال.

سجل حجز المسافرين PNR (*Passenger Name Records*) هي المعلومات التي يتم جمعها من المسافرين عبر الجو في نظام الاستخبارات الأوروبي، مثل اسم المسافر، وتواريخ ومسار الرحلة، والعنوان وأرقام الهاتف،

---

peuvent être combinées»: v. G29, avis sur la publicité comportementale en ligne, 22 juin 2010, adresse:
www.cnpd.public.lu/fr/publications/groupeart29/wp171_en.pdf.

[1] L. Bygrave, « Data Protection Law, Approaching Its Rationale, Logic and Limits », 2002, 316.

ووسائل الدفع المستخدمة، ورقم بطاقة الائتمان، ووكالة السفر، ورقم المقعد، والطعام المفضّل، ومعلومات عن الأمتعة[1]. وقد ظهرت أول أنظمة استغلال واسعة النطاق لهذه البيانات في أعقاب اعتداءات نيويورك في 11 سبتمبر 2001. بالفعل إن حفظها يسمح على سبيل المثال لمصالح الدولة بتتبع تواريخ تحركات الشخص الذي يتم اختياره تلقائيا لمزيد من الفحص.

وفي هذا الاتجاه، يرتبط جمع بيانات سجل حجز المسافرين PNR ارتباطا وثيقا باحترام العديد من الحريات الأساسية التي يحميها الميثاق الأوروبي، ولا سيما الحق في حماية حرمة الحياة الخاصة (المادة 7)، والحق في حماية البيانات الشخصية (المادة 8)، وحرية المبادرة الاقتصادية (المادة 16) أو مبدأ عدم التمييز (المادة 21). ويبدو أن الجانب المتعلق بحرمة الحياة الخاصة وحماية البيانات الشخصية هو الاكثر تضررا. تنتج الرهانات من حقيقة أن الأمر يتعلق بجميع البيانات التي يرسلها الركاب لشركات الطيران عند حجز رحلة والتي تسمح بإجراء تقييم للمخاطر التي يشكلها بعض الأشخاص، وجمع وإقامة صلات بين الأشخاص المعروفين وغيرهم ممن ليسوا كذلك. وبهذا المعنى فإنها تشكل أداة ضرورية لمكافحة الإرهاب والأشكال الخطيرة للجريمة المنظمة العابرة للحدود، وللتحقيقات والمتابعات القضائية في هذا المجال. ويصدق ذلك بصفة خاصة لأن معظم الأنشطة المتصلة بالجريمة المنظمة والإرهاب تنطوي في

---

[1] La définition des PNR retenue par les textes européens est la suivante: « le dossier de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens adhérents qui assurent les réservations pour chaque voyage réservé par une personne ou en son nom, que le dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs ou des systèmes équivalents offrant les mêmes fonctionnalités » (art. 2 de la proposition de dir. ci-dessous visée).

الوقت الراهن على أسفار دولية. وتتراوح هذه الأنشطة من الاتجار بالبشر والمخدرات، بما في ذلك وصول الإرهابيين إلى معسكرات تدريب خارج الاتحاد الأوروبي. وللتصدي لهذا التهدي د، وبالنظر إلى إلغاء الضوابط الحدودية الداخلية بموجب اتفاقية شنغن، فإن الهدف من السياسة الأوروبية المتبعة هو الوصول إلى المعلومات المطلوبة عن الأشخاص من وقت الحجز، قبل سفرهم، لتحديد الأفراد المشتبه فيهم حتى قبل وصولهم إلى المطار.

وفي هذا السياق، وبالنظر إلى تزايد مخاطر المراقبة الإلكترونية الشاملة وأساليب التحقيق التطفلية الناتجة عنها، يبدو من الضروري تأكيد أولوية سيطرة الانسان على تكنولوجيا المعلومات، ولا سيما في مجال الأمن العمومي.

الفصل ثاني

حماية الحريات العامة على الانترنت في مواجهة المراقبة الرقمية

القواعد القانونية الوقائية لحماية الحريات العامة.

إن المخاطر الجديدة التي تستهدف الحرّيات العامة دفعت العديد من الدول – كما رأينا – لوضع تشريعات إبتداء من السبعينات، و تضمنت قواعد إدارية و مدنية و جنائية من أجل حماية الحقوق و الحرّيات الأساسية. كما أن هذه المخاطر، وما يتفرع عنها من مخاطر أخرى، كتلك الناتجة عن معالجة البيانات في شبكات الكمبيوترات المربوطة ببعضها البعض و التي تتيح تبادل المعلومات بين المراكز المتباعدة و المختلفة من حيث أغراض تخزين البيانات بها، كانت محل اهتمام دولي و اقليمي و وطني أفرز قواعد و مبادىء تتفق و حجم هذه المخاطر.

لقد كفلت التشريعات و الوثائق، السابق عرضها، الحق في المعلومات و حرية تدفقها و انسيابها، و الحق في الحياة الخاصة و مبدأ عدم الإعتداء على البيانات الشخصية.

و شملت قواعد حماية حياة الأفراد الخاصة من مخاطر جمع و تخزين و معالجة و استخدام هذه البيانات و التي يتم جمعها من قبل هيئات و مراكز المعلومات سواء في القطاع الحكومي أو القطاع الخاص.

لقد تبنى مجلس أوروبا – الاتفاقية رقم 108 – والتي تشكل أهمية خاصة، بالنظر إلى أنها تفرض على الدول الموقعة الالتزام بإعتماد قانون يتضمن مبادئ الاتفاقية و ينص على عقوبات و أشكال الطعون، وشكلت هذه الاتفاقية أول أداة قانونية دولية تسمح بالتمتع بحق ملزم. من جانبها تركت الأمم المتحدة المبادرة التشريعية للدول، مع الاعلان عن 10 "مبادئ توجيهية لتنظيم الملفات المعالجة

آليا و التي تتضمن بيانات شخصية "[1]. دون تقديم تعريف دقيق، يشمل مع ذلك قرار الأمم المتحدة النقاط الرئيسية الموجودة في قانون المعلوماتية و الحريات الفرنسي، و هي: مبدأ النزاهة و المشروعية في جمع ومعالجة البيانات، و مبدأ الدقة ومبدأ الغرض، اطلاع الأشخاص المصرح لهم (ولا يوجد حق في معارضة المعالجة)، ومبدأ الأمن أو كذلك تعيين سلطة مراقبة. ومع ذلك و نظرا للطابع التصريحي البحت و غير الملزم لهذه المبادئ، كان علينا انتظار التدخل التشريعي للاتحاد الأوروبي و بروز نص دولي ملزم للدول الأعضاء على حد السواء.

ثم وفي خطوة متطورة على المستوى التشريعي الاقليمي، بل وذات أثر عالمي، أصدر الاتحاد الأوروبي الأمر التشريعي رقم 95/46/CE الخاص بحماية البيانات ونقلها عبر الحدود في 24 أكتوبر 1995، والذي كان نتيجة لعمل شاق دام قرابة عشر سنوات. و قد مثل مرحلة جديدة في اعادة تنظيم خصوصية المعلومات أدت الى اعادة وضع العديد من دول أوروبا تشريعات جديدة او تطوير تشريعاتها القائمة في هذا الحقل، بل أثّر فيما تضمنه من معايير في حقل نقل البيانات خارج الحدود لدرجة سعي العديد من دول العالم خارج النطاق الاوروبي الى التأقلم مع ما قرره هذا الأمر التشريعي.

أخذ الأمر التشريعي الأوروبي رقم 95/46/CE بعين الاعتبار تجميع كل أنواع البيانات تحت ستار الأنظمة الأمنية المتعلقة بوسائل التعريف الإلكتروني: هندسة اليد و بصمات الأصابع و الصوت و الوجه و قزحية العين، الخ و على الرغم من قيمتة القانونية الثابتة، فإن النص الأوروبي يصطدم بضرورة الحفاظ على سيادة كل دولة من الدول الأعضاء تجعله لا يشمل جزءا كبيرا من مجالات

---

[1] Rés. n° 45/95, AGNU, 14 déc. 1990, relative aux principes directeurs pour la réglementation des fichiers personnels informatisés.

معالجة البيانات، بما فيها المتعلقة بالأمن العام، و الدفاع عن أمن الدولة أو مكافحة الجريمة – تدخل هذه المجالات في الاطار التنظيمي الوطني.

و تضمنت هذه التشريعات في غالبيتها قيودا على نقل البيانات خارج الحدود إلى حدود أخرى، فقررت بعضها وجوب الحصول على تصريح بذلك، و اشترطت بعضها تسجيل هذه البيانات قبل نقلها، و أخرى ربطت الموافقة على النقل بتوفر تصريح بنشرها أولا داخل الدولة قبل نقلها.

وأوجبت هذه التشريعات تحديد الغرض الذي من أجله يتم جمع هذه البيانات و خزنها و معالجتها و استخدامها، والمدة المحددة لحفظها بالنظر إلى غرض الإستخدام، و أوجبت عدم إفشاء هذه البيانات وحماية معالجتها الآلية في نظم المعلوماتية، وقررت مبدأ الإنفتاح القاضي بإعلان السياسة العامة للتعامل مع هذه البيانات، وقررت مبدأ المشاركة الفردية لأصحاب البيانات بما يكفل الوصول إليها والتعرف والرقابة عليها وحق تعديلها وطلب حذفها إذا كانت غير صحيحة[1].

وانطوت هذه التشريعات على نصوص تقيم المسؤولية الجزائية للمنوط بهم التعامل مع هذه البيانات عن أي فعل من هذه الأفعال المتعارضة مع سيرتها واستخدامها المشروع والأسس الشكلية لمعالجتها.

ونظمت أخيرا القواعد الخاصة بسلطة إنفاذ القانون و مراقبة البيانات، ولو أردنا أن نقف أكثر على قواعد الحماية فإننا نجد أنها انطوت على نص يقرر الحق في الحياة الخاصة دون وضع تعريف لهذا الحق كما أسلفنا، و تتفاوت التشريعات في إقرار هذا الأصل بين النص الصريح، أو بتقرير حظر كل اعتداء على الحياة الخاصة و الشخصية.

---

[1] Pierre KAYSER, La protection de la vie privée par le droit, Economica / Presses universitaires d'AixMarseille, 3° éd., 1995 p.276.

أما بشأن مبدأ حماية البيانات الشخصية من المعالجة الآلية، فقد جرى النص عليه كأصل عام في التشريعات التي عالجت حماية الحياة الخاصة من مخاطر المعلوماتية – التشريعات الشمولية – كالتشريع الفرنسي مثلا (قانون رقم 17-78 لعام 1978 الخاص بالمعالجة الإلكترونية)، أما التشريعات التي تناولت حماية الخصوصية عموما دون سن تشريع خاص – التشريعات القطاعية _ كالتشريع الأمريكي فلم تتضمن مثل هذا النص.

ففي القانون الفرنسي المذكور تنص المادة الأولى على أن " المعالجة الإلكترونية يجب أن تكون في خدمة المواطن، و لا يجب أن تحمل أي اعتداء على شخصية أو حقوق الإنسان أو الحياة الخاصة أو الحريات الفردية أو العامة".

كما نصت قواعد الحماية على قواعد موضوعية و شكلية لجمع و استخدام البيانات الشخصية، كتحديد الغرض وجهة الجمع و المعالجة و المدة اللازمة لتحقق الغرض من تجميع البيانات، وأوجه الإستخدام، و توفير وسائل الأمن التقنية و تحديد الأشخاص المسموح لهم الإطلاع على البيانات، والخضوع لرقابة الهيئات الموكل لها بحكم القانون الرقابة على جمع و معالجة و نقـــــل واستخدام البيانات الشخصية، والواقع أن هذه القيود تمثل القواعد و المبادىء المقررة لدى المنظمات و الهيئات الدولية، خاصة الأوروبية.

وأفردت قواعد الحماية قواعد اجرائية بشأن حق الفرد في الوصول والاطلاع والتعديل والالغاء على البيانات الخاصة به، و هي القواعد التي تعد اطارا لتفعيل مبدأ المشاركة الفردية، بما في ذلك بيان القيود و مقتضيات تنظيم هذا الحــق.

و نصت على أحكام خاصة بشأن مسؤوليات جهات المعالجة والقائمين عليها و مسؤوليات الغير وبصورة عامة تقرير قواعد المسؤولية المدنية والجزائية وأحيانا السلوكية بالنسبة للموظفين.

و الواقع أن قيام أنظمة المعالجة الآلية للبيانات الشخصية وتجنب قدر الامكان أخطارها على الحياة الشخصية، يقتضي وضع قواعد و مبادىء تلتزم بها هذه الأنظمة و تكون بمثابة ضمانات وقائية لحرمة الحياة الخاصة، ومن تشريعات الدول الأجنبية والوثائق الدولية يمكن استخلاص ثلاثة مبادىء أساسية يمكن من خلالها أن نكفل التوازن بين نشاط أنظمة معالجة البيانات الشخصية وتطورها، و بين حماية الحياة الخاصة، وهذه المبادىء[1] هي: مبدأ الأمن (مطلب أول)، و مبدأ المشروعية(مطلب ثاني)، ومبدأ توفير الطمأنينة (مطلب ثالث).

مبدأ الأمن.

إن تحقيق مبدأ الأمن بالاشــراف و الرقابة غير المباشرة للدولة على انشاء الأنظمة المعلوماتية و مباشرتها لنشاطها يقتضي توافر مسألتين، الأولى ايجاد جهة مستقلة (فرع أول) و الثانية أن تكون لها صلاحيات واسعة بما يكفل لها ممارسة دورها الاشرافي والرقابي بشكل يكفل التطبيق الدقيق لقانون المعلومات (فرع ثاني).

سلطات الرقابة.

يتعلق الأمر هنا بدراسة طبيعة سلطات الرقابة المكلفة بتطبيق القوانين المتعلقة بحماية البيانات الشخصية، فمن الضمانات الوقائية الخاصة بتفادي ما هو محتمل من أخطار الأنظمة المعلوماتيــة على الحياة الشخصية للأفراد، أن يكون للدولة رقابة و اشراف غير مباشر على قيام هذه الأنظمة بنشاطها، و يكون ذلك من خلال ايجــاد جهة متخصصة، مكونة من مجموعة من الفنيين المتخصصين

---

[1] بولين انطونيوس ايوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية (دراسة مقارنة)، لبنان. منــشورات. الحلبــي. الحقوقية، 2009، ص449.

في المعلوماتية والقانونيين الأكفاء، تكون لها القدرة على التوفيق بين ضرورة وجود هذه الأنظمة و تطورها و ضمان حماية الحاة الشخصية للأفراد.

و يؤكد الفقه[1] على عدم كفاية وجود قانون للمعلومات لحماية الحياة الشخصية دون وجود جهة متخصصة ذات طبيعة متميزة للاشراف و الرقابة على قيام الأنظمة المعلوماتية و ممارستها لنشاطها، كون التوفيق بين تطور الأنظمة المعلوماتية و ضمان حماية الحياة الشخصية يقتضي إضافة إلى وجود قانون ينظم المبادئ الخاصة بإنشاء نظم المعلومات وفي قيامها بنشاطها، وجود جهة ذات طبيعة متميزة تتولى مراعاة التطبيق الصحيح للقانون تكون مهمتها الإشراف و الرقابة على إنشاء نظم المعلومات و تقديم الإستشارات والتعليمات المرنة التي تحقق تطور المعلوماتية و الإستفادة منها، في الحدود المرسومة في القانون مع ضمان حقوق الأفراد في الحياة الشخصية.

كما تنبهت المنظمة العالمية للثقافة و العلوم (UNESCO) في اجتماعية الذي عقد في العاصمة الفرنسية باريس في الفترة من 19 – 23 كانون الثاني 1970 إلى أن استخدام الكمبيوتر لما له من قدرة فائقة على جمع و تخزين و معالجة البيانات و إيصالها إلى المستخدم في فترة زمنية قصيرة جدا يهدد الحياة الخاصة للأفراد، و أن هذا الأمر يقتضي وجود جهة تتولى الرقابة على هذه الأنظمة[2]. وقد أكدت محكمة العدل الأوروبية في كثير من المناسبات على استقلالية هذه الهيئة في العديد من قرارتها[3].

---

[1] Jean et Frayssinet Jean, Les libertés individuelles à l'épreuve des Ntic, Pul, 2001, P.75.

[2] أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية، القاهرة، 1994، ص83.

[3] Voir les arrêts Commission c/ Allemagne, aff. C-518/07 ; Commission c/Autriche, aff. C-614/10 ; Commission c/Hongrie, aff. C-288/12.

و نظرا لأهمية وجود جهة متخصصة في الإشراف و الرقابة على إنشاء أنظمة المعلومات الإسمية و ممارستها لنشاطها، فقد حرص بعض من الدول التي سنت القوانين الخاصة بالمعلوماتية على إيجاد مثل هذه الجهة[1]، كألمانيا و فرنسا، بالرغم من وجود اختلاف بشأن تسمية هذه الجهة أو القائمين بعملها الإشرافي أو الرقابي، ففي القانون الفرنسي الصادر في 16 كانون الثاني 1978 المتعلق بالمعلوماتية والحريات هذه اللجنة الوطنية للمعلومات و الحريات[2] و المكونة من سبعة عشر عضوا، بينما في القانون الألماني يتولى الرقابة على تطبيق قانون المعلومات المفوضون. و هناك نوعين من المفوضين[3]:

1 – المفوض الفدرالي لحماية البيانات في القطاع العام (Commissioner for Data Protection Federal).

2 – مكتب حماية البيانات في القطاع الخاص (Data Protection Officer)

والواقع أن النموذج الفرنسي فيما يتعلق بالجهة التي تتولى الإشراف و الرقابة على إنشاء نظم المعلومات و قيامها بنشاطها يعتبر نموذج جيد، إذ أن كثرة عدد أعضاء اللجنة من الخبراء الفنيين المتخصصين في المعلوماتية و رجال

---

[1] بخلاف إنكلترا والولايات المتحدة الأمريكية، حيث لم يأخذ المشرع فيها بالرقابة التي تمارسها جهة متخصصة تتمتع باستقلال واسع في الرقابة السابقة على إنشاء نظم المعالجة الآلية للبيانات و على عملها اللاحق، بل إكتفى بالرقابة القضائية وفقا للقواعد العامة لحماية الحق، وبالتالي ليس هناك هيئة مستقلة لحماية الخصوصية. لكن قد نجد في الولايات المتحدة جهات متعددة تعمل على تطبيق القوانين القطاعية لحماية الخصوصية، و أما أهم جهتين على صلة بالخصوصية، هما: مكتب الادارة والميزانية ولجنة التجارة الفدرالية.

[2] Commission nationale de l'informatique et des libertés (CNIL): https://www.cnil.fr/

[3] https://www.bfdi.bund.de

القانون، و تولي جهات مختلفة مهمة اختيارهم، و استقلاليتهم في ممارستهم لمهامهم في الإشراف و الرقابة و عدم خضوعهم في عملهم إلا لرقابة القضاء، كل ذلك يوفر للجنة الوطنية للمعلوماتية و الحريات الفرنسية القدرة على الرقابة الدقيقة للتطبيق الصحيح لقانون المعلوماتية، من جهة، و يجعلها حيادية و يقوى دورها في حماية الحياة الشخصية في مواجهة أنظمة المعالجة الالية للبيانات الشخصية.

تجدر الاشارة أنه وبالاضافة إلى غياب قانون لحماية البيانات الشخصية، لا تتوفر أيضا المنظومة القانونية في الجزائر على هيئة لحماية الحقوق و الحريات الرقمية كما هو جاري به العمل دوليا.

فرع ثاني: صلاحيات جهة الاشراف و الرقابة.

ان فعالية دور الجهة المناط بها الاشراف والرقابة على انشاء نظم المعلومات وقيامها بنشاطها، وحتى تكون احدى الضمانات الوقائية لحماية الحياة الشخصية في مواجهة الانظمة المعلوماتية يتوجب ان تكون لها سلطات واسعة تمكنها من الاشراف و الرقابة السابقة و اللاحقة على انشاء انظمة المعالجة الالية للبيانات الشخصية.

أولا:الرقابة و الاشراف على انشاء نظام المعالجة الآلية للبيانات الشخصية.

ان وضع القواعد القانونية[1] التي تمنع انشاء نظم المعلومات دون المعرفة المسبقة للجهة المناط بها مهمة الاشراف و الرقابة و كذلك القواعد التي تمنح هذه الجهة سلطات واسعة في التدقيق في الوثائق الخاصة باقامة نظم المعلومات و

---

[1] Yves POULLET: Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information, Droit de l'Informatique, 1987, n.4.

التاكد من استيفاء الشروط و الضوابط المحددة قانون لانشاء هذه النظم، و من تناسب المعلومات المطلوب تجميعها و الهدف من انشاء نظام المعلومات، و تنبيه من يرغب في اقامة نظام للمعلومات بها يتوجب اتخاذه من الاجراءات و التامينات الفنية التي تتلاءم مع طبيعة النظام، و كذلك وضع القواعد التي من شانها ان تجعل جهة الرقابة و الاشراف مستقلة في قرارات الموفقة او الرفض لاقامة نظام المعلومات، و كل ذلك من شانه ان يوفر احدى الضمانات الوقائية لحماية الحياة الخاصة في مواجهة نظم المعالجة الالية للبيانات الشخصية.

و قد أخذ القانون الفرنسي المتعلق بالمعلوماتية و الحريات بمبدأ الاشراف و الرقابة السابقة على انشاء نظم المعلومات و إن كان قد فرّق بين اجراءات انشاء نظم المعلومات من قبل أشخاص القانون الخاص حيث يقتصر الأمر في هذه الجالة على اخطار اللجنة الوطنية للمعلوماتية والحريات بانشاء النظام، بينما يختلف الامر في حالة رغبة أحد أشخاص القانون الخاص العاملين لحساب الدولة، ففي هذه الحالة بتوجب القيام باجراءات الحصول على ترخيص بذلك[1].

و الواقع ان هذه التفرقة ليس الهدف منها الاعفاء من يرغب من اشخاص القانون الخاص في اقامة نظم للمعلومات من الرقابة و الاشراف السابق على انشاء النظام، بل الهدف هو عدم اثقال القطاع الخاص بالاجراءات الادارية و القيود التي تتنافى مع حركة التجارة فقط. أما من حيث وجوب توافر الشروط و الضوابط القانونية لانشاء نظام المعلوماتية فهي واحدة في الترخيص وفي الاخطار حيث يتوجب لانشاء اي نظام للمعلومات سواء من قبل اشخاص القانون الخاص او القانون العام تحديد الهدف من انشاء النظام و خصائصه والجهة التي

---

[1] Marie-Christine Piatti: Les libertés individuelles à l'épreuve des NTIC, PUL, 2002, P.144.

تمارس في مواجهتها حقوق الاستعمال و الاطلاع والتصحيح و نوعية البيانات التي يزمع تجميعها و الهدف منها و مصادر جمع هذه البيانات ومدة الاحتفاظ بها و الجهات التي تستفيد منها او يجوز لها استقبال المعلومات و طرق تحليل و معالجة البيانات و الضمانات الكفيلة بسلامة البيانات ومعالجتها و سريتها[1].

ثانيا: الرقابة و الاشراف اللاحق على انشاء نظم المعلومات.

ان الاشراف و الرقابة على نظم المعلومات كإحدى الضمانات الوقائية لحماية الحياة الشخصية في مواجهة نظم المعلومات ينبغي ان لا تقتصر على انشاء هذه النظم بل ينبغي ان تمتد الى ما بعد انشاء نظم المعلومات وذلك من خلال منح الجهة المناط بها مهمة الاشراف والرقابة السلطات اللازمة للايفاء بدورها الاشرافي الرقابي الوقائي و المتمثلة في موضوع التنفيذ الصحيح و الدقيق و كذلك في حق مراقبة مدى احترام الجهة القائمة بالمعالجة للهدف المحدد للنظام و التحقق من التزامها بالقانون و توجيه الانذار الى ذوي الشأن عند اكتشاف أي مخالفة و تلقي الشكاوي وابلاغ النيابة العامة عند مخالفة أحكام القانون والتأكد من ضمان القائم على نظام المعلومات للأفراد حق الاطلاع والتصحيح للبيانات و المعلومات دون أي معوقات.

في 2008 تلقت اللجنة الوطنية للمعلومات والحريات الفرنسية CNIL 4244 شكوى متعلقة بانتهاك القانون، 25% منها متعلق بمجال التجارة، 25% منها متعلق بمجال البنوك، 15% منها متعلق بمجال العمل، 10% منها متعلق بمجال الاتصال، و10% متعلق بمجالات أخرى مختلفة[2].

---

[1] Nidal El Chaer: La criminalité informatique devant la justice pénale, edition Sader, 2004, P.431.

[2] أنظر: COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 29 Rapport d'activité, Paris, La Documentation française, Paris, 2009.

مبدأ النزاهة والمشروعية[1].

ان ضمان حماية الحريات العامة للافراد في مواجهة نظم المعلومات يقتضي ان يكون مبدأ المشروعية هو الأساس الذي يقوم عليه نشاط هذه النظم أي ان تكون كل مرحلة من مراحل المعالجة الآلية للبيانات الشخصية قائمة على أساس مشروع بدءا من جمع و تسجيل البيانات وانتهاءا بايصال المعلومات المعالجة الى الغير على النحو الذي سيتم تناوله في الفروع الاربعة التالية:

مشروعية جمع وتسجيل البيانات الشخصية.

يكون الأساس الذي يقوم عليه جمع و تسجيل البيانات الشخصية مشروعا اذا كانت البيانات التي تمكنت الجهة القائمة على نظام المعلومات الوصول اليها، ثم تغذية جهاز الكمبيوتر بها بناءا على موافقة الشخص الذي تتعلق به هذه البيانات أو بناءا على نص في القانون في الحالات الاستثنائية التي لا يقتضي الامر فيها الحصول على موافقة الشخص.

فالبيانات الشخصية باعتبارها مرتبطة بشخص صاحبها – مثل اسمه وحالته الاجتماعية وموطنه وحالته الصحية ومعتقداته السياسية والفلسفية أو الدينية أو الانتماءات النقابية أو صحيفة سوابقه العدلية، رقم حسابه المصرفي، عنوان البريد الالكتروني و غيرها من المعلومات التي توصف بأنها حساسة و التي تسمح بصورة مباشرة أو غير مباشرة بتعريف الاشخاص الذي يجري جمع المعلومات عنهم – تتطلب الموافقة الخطية الصريحة من قبل الشخص المعني بها قبل

---

[1] أجمع الفقه على إستخدام مبدأ المشروعية، الذي هو ترجمة حرفية للمصطلح الفرنسي المقابل: Le principe de légalité للمزيد من التفصيل راجع:

-GARRAM Ibtissem, Terminologie juridique dans la législation algérienne, lexique Français, Arabe, ENAG, Alger, 1992, pp 171 et 176.

المباشرة بجمعها باستثناء بعض الحالات المنصوص عليها في القانون والتي لا تتطلب موافقة الشخص[1].

وفي هذا الإطار فقد نصت المادة 6 من التوجيه الأوروبي رقم 95/46 بتاريخ 24 أكتوبر 1995 المتعلق بحماية الأشخاص الطبيعيين في مواجهة معالجة البيانات ذات الطابع الشخصي وحرية تداول وانتقال البيانات[2]، على أن جمع المعلومات يجب أن يكون لغايات محددة وواضحة ومشروعة ولا يجوز استخدامها لاحقا بغرض مغاير للغايات التي من أجلها جمعت. وقد أضافت المادة المذكورة أن البيانات ذات الطابع الشخصي يجب أن تجمع بطريقة مشروعة.

بالإضافة إلى ذالك فان المادة 10 من التوجيه المذكور تنص على أنه وفي حال جمع المعلومات بصورة مباشرة من الشخص المعني، يتوجب أخذ الموافقة الصريحة من قبل هذا الأخير. والموافقة الصريحة تقتضي قبل كل شيء إعلام الشخص المنوي جمع المعلومات عنه، وإعلامه أيضا بالطابع الإلزامي أو الاختياري للأجوبة، وبالنتائج المحتملة وفي حال عدم الإجابة، وبهوية الأشخاص الماديين أو المعنويين الذين ستؤول إليهم المعلومات المجمّعة، وأخيرا بحقهم في الوصول إلى هذه المعلومات وفي تصحيحها.

ويعني ذلك أن يتوفر نوعا من النزاهة في عملية جمع البيانات الشخصية فلا تجمع بأية طريقة خادعة أو غير أخلاقية أو غير مشروعة وبالتالي يتوجب على كل من يتولى معالجة معلومات شخصية، بأن يلتزم تبعا

---

[1] Jacques Robert, Jean Duffar Droits de l'homme et libertés fondamentales, Montchrestien, 1999, p.50.

[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050.

لصفته هذه، تجاه الأشخاص المعنيين بها، بأن يأخذ كافة الاحتياطات المجدية من أجل توفير أمن المعلومات، لاسيما الحـــؤول دون تحريفها أو تعيّبها أو وصولها إلى الغير غير المرخص لهم بالاطلاع عليها. وتكمّل المادة 11 أنه في حال جمع المعلومات بصورة غير مباشرة، يتوجـب علن المسؤول عن المعالجـة إعـلام صاحـب العلاقـة عند أول بث لهذه المعلومات أو عند تسجيلها أو إرسالها إلى شخص ثالـث.

واستنادا لمـا تقدم تعتبـر عمليـات الجمـع والتسجيـل للبيانات الشخصية غير مشروعـة في الحالات التالية:

أولا: الموافقة غير الصحيحة.

إن الموافقـة التي تصدر من الشخص لتسجيل البيانات المتعلقـة به، دون تنبه أو تبصر على النحو السابق بيانه، تنفي أساس المشروعية في عمل نظام المعلومات، وتجعل من قيامه بجمع هذه المعلومات عملا غير مشروع تقوم معه مسؤوليته القانونية[1] ويدخل في ذلك الحصول على البيانات بطريق الغش والتدليس[2]. فإذا كانت الأسئلة التي تتضمنها الاستمارة الذي يفترض على الشخص الإجابة عليها من اجل الحصول على ميزة معينة أو وثيقة، لاتتناسب مع ما يتوجب أن يدلى به من بيانات لهذا الغرض، بل تتعدى ذلك بكثير، فاضطر الشخص الى إعطاء البيانات الخاصة به، فهذا الأمر يجعل من موافقة هذا الشخص موافقة غير صحيحة، كون عدم التناسب ينطوي على غش يعيب الارادة.

---

[1] Frédéric-Jérôme Pansier: La criminalité sur internet, éd. Puf, 2000, p.140.

[2] Georges Kellens: Revue internationale de criminologie et de police technique, 1991, n.2, p.243.

كما ان الموافقة تكون غير صحيحة اذا كانت قائمة على ارادة معيبة بسبب التدليس أو الخداع، فاذا صدرت الموافقة بناء على ما عرضته الجهة القائمة على نظام المعلومات من وعود كانت الدافع إلى أن يقوم الشخص بتقديم بيانات خاصة به، ما كان ليقدمها لولا هذه الوعود، ثم تبين عدم صحة هذه الوعود، في هذه الحالة تكون موافقة الشخص غير صحيحة لما أصابها من تأثير الخداع الناتج عن الوعود الكاذبة.

ثانيا: عدم موافقة الشخص المتعلقة به البيانات.

يعد جمع وتسجيل البيانات الشخصية دون موافقة صاحبها عملا غير مشروع تقوم بموجبه المسؤولية القانونية في مواجهة الجهة القائمة بالمعالجة[1]، فاعتراض الشخص على تسجيل ما يخصه من بيانات شخصية باعتبارها من أسرار حياته الخاصة التي لا يجوز للغير الاطلاع عليها لتعلقها بشخصيته فان هذا الاعتراض ينفي عن عملية الجمع و التسجيل للبيانات صفة المشروعية إلا إذا أجاز القانون تسجيل هذه البيانات بصورة استثنائية[2].

ومن الاستثناءات على تسجيل البيانات في ذاكرة الكمبيوتر بموجب القانون ما نصت عليه المادتان 32 و 33 من القانون الفرنسي المتعلق بالمعلوماتية والحريات والذي أجاز بموجبها للكنائس والتنظيمات والجامعات ذات الصبغة الدينية أو السياسية أو النقابية بتسجيل البيانات المتعلقة بأعضائها ومعالجتها آليا.

---

[1] Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (article 226-16 à 226-24 du code pénal), Jurisclasseur Pénal Code, fascicule 20, 2006, 50 p.

[2] MAISL HERBERT, Communications mobiles, secret des correspondances et protection des données personnelles, LPA, 21 juin 1995, n.74.

ويرد الفقه[1] هذا الاستثناء إلى الموافقة الضمنية لأعضاء هذه الجماعات والتنظيمات، ففي القبول في الانضمام إلى هذه الجمعيات والتنظيمات موافقة ضمنية على قيد البيانات التي يتوجب توافرها للأعضاء في السجلات الخاصة بها، والتي منها نظم المعلومات.

ومن الاستثناءات أيضا المصلحة العامة[2]، إلا أن المشرع الفرنسي لم يجعل تقدير المصلحة العامة للجهة القائمة على نظام المعلومات، بل للجنة الوطنية للمعلومات و الحريات والتي تقدر هذه المصلحة على أساس أهمية البيانات المراد تسجيلها وكذلك الهذف من المعالجة الآلية والمخاطر التي تهدد حرية الأشخاص نتيجة لمعالجة تلك البيانات.

وقد أثير الخلاف بشأن مدى جواز إقامة نظام للمعلومات الشخصية لمرضى الايدز حتى يمكن حصرهم ووضع الضوابط للتعامل معهم كون الأمر هنا يحتوي على تعارض بين حماية الحياة الخاصة وبين ضرورات تحقيق المصلحة العامة المتمثلة في مكافحة مرض الايدز والوقاية من مخاطره والرأي الغالب قد غلب حماية الحياة الخاصة ورفض اقامة مثل هذا النظام لأن الامر سيجعل من هؤلاء المرضى طائفة من المنبوذين في المجتمع، في الوقت الذي يمكن اتخاذ وسائل أخرى لمكافحة هذا المرض بعيدا عن نظم المعلومات[3].

---

[1] محمود عبد الرحمن محمد: نطاق الحق في الحياة الخاصة، ط1، منشورات دار النهظة العربية، القاهرة، ص164.

[2] Louise Cadoux: Les reponses technologiques. LPA, 10/11/1999, n.224, p.47.

[3] Pierre KAYSER, La protection de la vie privée par le droit, Economica / Presses universitaires d'AixMarseille, 3° éd., 1995 p.256.

والاستثناء الثالث يتعلق بحق وسائل الاعلام المختلفة في جمع وتسجيل وتخزين ومعالجة البيانات المتعلقة بالحياة الخاصة ويهدف هذا الاستثناء إلى ضمان حرية وسائل الاعلام في التعبير ونشر الاراء المختلفة، وكذلك حق الجمهور في الاعلام الذي لا يمكن أن يتحقق إلا إذا منحت وسائل الاعلام المختلفة الحرية في التعبير فكان لها استثناءا تسجيل وتخزين ومعالجة المعلومات المختلفة المتعلقة بالأصل العرقي والآراء السياسية والفلسفية والدينية والانتماء النقابي للشخص.

ثالثا: جمع وتسجيل البيانات الشخصية دون علم الشخص.

يعتبر جمعا وتسجيلا غير مشروعا الجمع الذي يتم دون علم الشخص وفي غير الحالات التي يجيزها القانون كالبيانات التي يتوصل إليها النظام عن طريق التنصت على الهاتف أو التسجيل منه، أو بناءا على تجميع المعلومات من نظم المعلومات المختلفة عن طريق ربط نظم المعلومات المنشئة لتحقيق أغراض مختلفة بعضها ببعض، أو عن طريق استخدام الكعك المحلى[1] (Cookies) الذي يوضع على الاسطوانة الصلبة لجهاز الكمبيوتر الخاص بالمستخدم دون علمه فيسمح برسم شخصيته وهوياته – كما أن شبكة الانترنت ليست بمنأى عن هذه الامكانيات في جمع البيانات والمعلومات وفي مراقبتها. لا بل إنها تهدد بتشديد المخاطر الناجمة عنها وبمضاعفتها، لاسيما إذا أدركنا ان كل إتصال بالانترنت يمكن أن يترك أثرا ما، حتى ولو لم يتفطن مستخدم الشبكة دوما إلى ذلك.

فمن جهة أولى تجري أرشفة جميع المشاركات في منتديات المحادثة وفي المجموعات الاخبارية، داخل قواعد بيانات ضخمة يتم الدخول إليها بحرية. أما

---

[1] مدحت رمضان: الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية، 2001، ص98.

محركات البحث، فهي تحتفظ بطلبات البحث عن المعلومات التي يجريها مستخدموا الشبكة لآجال متفاوتة[1].

في الويب العالمي يترك كل إتصال على الاقل، توقيت حصوله، والصفحة التي جرى تفحصها وعنوان موقع الكمبيوتر الذي أجرى هذا الاتصال[2].

ويمكن أن تذهب المراقبة في شبكة الانترنت إلى أبعد من ذلك إذ يمكن الحصول أحيانا على عناوين مستخدمي البريد الالكتروني والموزعات التي انطلقت الرسائل عبرها[3].

كما أن المواقع التي تزاول التجارة الالكترونية مباشرة عبر الشبكة، تحتفظ بالبيانات المتعلقة بالصفقات التي يجريها المتسوقون معها وبمعلومات شخصية حول هؤلاء.

ينسحب ذلك على الوسطاء والاشخاص الثالثين المصادقين ومختلف الهيئات والمراجع التي تؤدي دور الوساطة بين التاجر و زبائنه[4]. وفي الواقع إن غالبية هذه المواقع، تحمل زوارها، من مستخدمي الشبكة، على ملء إستمارات إلكترونية تحوي معلومات شخصية عنهم، و ذلك قبل أن تسمح لهم بالنفاذ إلى الخدمة المقصودة.

وأيا تكن الطريقة التي تجمع المعلومات بواسطتها، يمكن الجزم بأن إستخدام شبكة الإنترنت يترك بيانات شخصية خلفه عن مستخدميها، يبقى جزءا كبيرا من هذه المعلومات غير مستثمر في ذاكرات أجهزة الكمبيوتر الموصولة بها. في حين

---

[1] على سبيل المثال يحتفظ محرك البحث Altavista بطلبات البحث عن المعلوماتلمدة شهر كامل.

[2] طوني عيسى: التنظيم القانوني لشبكة الانترنت، المرجع المشار إليه سابقا، ص34.

[3] http://www.edt.org

[4] Alain Bensoussan: le commerce electronique, op. cit. 1998, p.50.

تستغل أجزاء لا بأس بها في رسم صور جانبية عن مستخدمي الشبكة، وبالتالي فإنها تستغل في مراقبتهم[1].

إن كل ما تقدم، وغيرها من الطرق السابق تناولها في الفصل الأول من هذا البحث، تشكل خطرا على الحياة الشخصية لاسيما إذا إستغلت المعلومات و البيانات المجمعة لغايات وأغراض مختلفة بدون رضى أصحابها وحتى بدون علمهم أنها قد جمعت أصلا.

مشروعية تخزين البيانات الشخصية.

إن مشروعية تخزين البيانات الشخصية يقتضي أن يكون التخزين يتناسب مع الهدف من إقامة نظام المعلومات[2]، وأن يكون لمدة محددة، وأخيرا العمل على عدم وصول الغير إلى البيانات و المعلومات المختزنة، وسوف يتم إيضاح ذلك في مايلي:

أولا: مبدأ تحديد الغرض من جمع البيانات[3].

يشكل مبدأ تحديد الغرض سببا لوجود أي نظام لمعالجة البيانات الشخصية. ويشكل الهدف المحدد عند انشاء أي نظام لمعالجة البيانات. في هذا الصدد يبرر هذا المبدأ أيضا وجود الخصائص الرئيسية لأي نظام لمعالجة البيانات (نوعية

---

[1] Sophie Coignard. internet. Le reseau qui fait peur aux services secrets. Le Point, 29 juillet 1995, n.123.

[2] Robert Charvin et Jean-Jacques Sueur: Droits de l'homme et libertés de la personne, 2eme edition, Litec, 1997, p.123.

[3] أنظر: Duaso-Calès, Rosario, Principe de finalité, protection des données et secteur public: la gouvernance des structures en réseau, Thèse de doctorat, 14 octobre 2011, Universités CRDP-Montréal-Paris II.

البيانات، المدة...) وبالتالي أصبح هذا المبدأ من أهم المعايير التي تستخدمها سلطة الرقابة من أجل تقدير مشروعية وشرعية مشاريع المعالجة التي تنظرها[1].

إن الفكرة الأساسية لمبدأ تحديد الغرض هي التي تحظر "الترابط الشامل" بين جميع السجلات الالكترونية الموجودة في الادارة العمومية[2].

ويقصد بالتناسب بين تخزين البيانات والهدف من إقامة نظام معالجة البيانات تكون البيانات المراد تخزينها متناسبة وضرورية للهدف المقصود من نظام المعالجة[3]، وأن يكون الهدف مرتبطا بمهمة ووظيفة الجهة القائمة على نظام المعالجة مع مراعاة مقتضيات احترام الحياة الخاصة للأفراد أي أن تكون البيانات المطلوب تخزينها تكفي لتحقيق الغرض من نظام تسجيلها و تخزينها دون زيادة عن هذا الغرض[4]. فعلى سبيل المثال المعلومات عن المرضى العقليين، إذا تم فيه تسجيل و تخزين بيانات عن الحالة الإجتماعية أو الدينية لهؤلاء الأشخاص، فإن هذه البيانات تنفي صفة المشروعية للتخزين كون هذه البيانات لا تتناسب مع الغرض من النظام بل تزيد عن الغرض الذي من أجله يراد تسجيلها.

ثانيا: تخزين البيانات لمدة محددة.

إن مشروعية تخزين البيانات الشخصية يقتضي أن يكون التخزين مؤقتا و ليس أبديا، كون الحق في الحياة الخاصة من الحقوق الملازمة للإنسان و التي تعتبر إحدى وسائل حمايتها دخولها في طي النسيان وهو الأمر الذي يحتاج إلى

---

[1] Isabelle DE LAMBERTERIE et Henri-Jacques LUCAS (dir.), Informatique, libertés et recherche
médicale, Paris, CNRS Éditions, 2001, p. 79.

[2] Duaso-Calès, Rosario, Principe de finalité, protection des données et secteur public: la gouvernance des structures en réseau, Thèse de doctorat, 14 octobre 2011, Universités CRDP-Montréal-Paris II, p.16.

[3] Antoine LATREILLE: La protection juridique des bases de données électroniques, Revue Internationale du Droit d'Auteur, n°164, avril 1995.

[4] أنظر: CEDH, 17 déc. 2009, req. n° 28164/05, § 62.

فعل إيجابي في حذف البيانات أصبح يشكل الإستثناء وليس القاعدة[1]. ولهذا فإن التخزين المؤقت للبيانات الشخصية هو إحدى الضمانات الوقائية لحماية الحياة الخاصة لأن الإحتفاظ و لمدة طويلة ببيانات و معلومات قابلة للتغير و التطور يؤدي استرجاعها بعد مدة طويلة من الزمن إلى الإضرار بصاحبها.

و يرى الفقه[2] أن المدة القصوى للاحتفاظ بالبيانات المختزنة هو مدة التقادم، و يمكن أن تقل مدة الاحتفاظ عن هذه المدة إذا لم يكتمل التقادم، أي أن تكون المدة في هذه الحالة بين سنتين و خمس سنوات. وهذه المدة تسري على كافة البيانات الشخصية، باستثناء البيانات التي يمكن أن تعدل أو تغير بمرور الزمن كالاسم و تاريخ الميلاد.

ثالثا: توفير الضمانات الفنية.

إن الاحتفاظ بالبيانات و المعلومات في ذاكرة جهاز الكمبيوتر و الذي يشكل أحد المخاطر على الحياة الخاصة نظرا لإمكانية الوصول إليها، و بالتالي فإن مشروعية هذا التخزين و الاحتفاظ يقتضي التزام الجهة القائمة على نظام المعلومات بتوفير الوسائل الفنية للحيلولة دون وصول أي فرد إلى البيانات و المعلومات المختزنة في النظام[3]، على النحو الذي تم تناوله سابقا.

---

[1] Antoinette Rouvroy, « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? », in Stéphanie Lacour (dir.), La sécurité de l'individu numérisé. Réflexions prospectives et internationales, Paris, L'Harmattan, 2009, p. 2.

[2] محمد عبد المحسن المقالع: حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسب الآلي، الكويت 1992، ص192.

[3] المادة 34 من قانون المعلوماتية والحريات الفرنسي.

مشروعية تشغيل البيانات.

إن مشروعية العمليات التي تتم آليا بهدف استغلال البيانات عن طريق الربط والتقريب ودمج بيانات أخرى و تحليلها للحصول على معلومات ذات دلالة خاصة يقتضي[1]:

أولا: عدم الاعتماد على بيانات شخصية غير دقيقة أو غير صحيحة بهدف الحصول على حكم أو تقييم لشخصية الإنسان، كون النتائج أو الأحكام التي يمكن الوصول إليها من عملية دمج و تحليل و معالجة هذه البيانات حتما ستكون غير صحيحة، و هذا من شأنه إلحاق ضرر بالغ بالشخص.

ثانيا: عدم استخلاص حكم أو تقييم لشخصية الإنسان من خلال البيانات التي سبق جمعها و تخزينها فقط دون البحث في الظروف والأحوال الأخرى التي تخص كل حالة على حدى.

مشروعية نقل وإيصال المعلومات إلى الغير.

إن مشروعية نقل وإيصال المعلومات إلى الغير باعتبارها الوظيفة الأساسية لنظم المعلومات يقتضي من جهة عدم نقل أو تداول المعلومات خلافا للهدف من إقامة نظام المعلومات الشخصية[2] ويتحقق ذلك إذا كان الشخص على علم بالغرض من إقامة نظام المعلومات الشخصية وغرض الإدلاء بالبيانات وتسجيلها وخزنها وبالأشخاص الذين سيستفيدون من هذه البيانات الخاصة به.

---

[1] MEILLAN, Eric: Les menaces à la sécurité des systèmes d'information.: la réponse des institutions françaises, Revue Internationale de Police Criminelle, Lyon, V.430 (Mai-Juin 1991), p.30-33

[2] نبيل مغبغب: مخاطر المعلوماتية والانترنت، دار النهضة العربية.، القاهرة، 1997، ص249.

إن موافقة الشخص في ظل هذه الظروف تفيد ضمنا الموافقة باستخدام هذه المعلومات ونشرها في الحدود اللازمة لتحقيق غرض النظام[1]، وتنسحب هذه الموافقة إلى النقل والتداول المتوقع في حدود الغرض من النظام[2] و لهذا يجب ان يكون نقل وايصال المعلومات الى الغير مشروعا ان يقتصر هذا النقل الى الغير بالغرض من النظام وعدم نقل وايصال المعلومات الى الاشخاص المتوقع اطلاعهم عليها طبقا للغرض من نظام المعلومات وبهدف الزام المعلومات الشخصية بعدم نقل وايصال المعلومات خلافا للغرض من إنشاء النظام حماية للحياة الخاصة للافراد في مواجهة توسع نظم المعلومات على أوسع مدى تحقيقا للربح المادي[3].

مبدأ مشاركة الأفراد.

من المبادئ الأساسية لحماية الحق في الحياة الخاصة في مواجهة نظم المعلومات الشخصية وضع القواعد القانونية التي تكفل للفرد قدرا من الاطمئنان

---

[1] حسني المصري: الكمبيوتر كوسيلة فنية لإنسياب المعلومات عبر الحدود الدولية وصور إستغلاله التجاري الدولي. ممؤسسة الكويت للتقدم العلمي، ط1، 1994، ص167-266.

[2] Cour de justice de l'Union européenne, 1er octobre 2015, aff. C-201/14, *S. Bara c/ Casa Națională de Asigurări de Sănătate et a.* L'arrêt de la CJUE rendu dans l'affaire S. Bara censure la pratique de l'administration roumaine consistant en la communication par l'administration fiscale à la Caisse nationale de sécurité sociale d'informations relatives aux revenus déclarés par des travailleurs indépendants, pour permettre le recouvrement d'arriérés de cotisations, sans que les personnes concernées aient été informées au préalable de cette communication. Une telle pratique est contraire au principe général de loyauté des traitements

[3] محمد عبد المحسن المقالع: حماية الحياة الخاصة للأفراد وضمانتها في مواجهة الحاسوب الآلي، الكويت، 1992، ص254.

على صحة ما يتم معالجته آليا من بيانات شخصية تتعلق به وعدم إفشاء ما يخصه من معلومات لا يرغب في الاطلاع عليها من قبل الغير و ذلك بمنحه الحق في الاطلاع على ما يتم تسجيله من بيانات و نتائج المعالجة الآلية لهذه البيانات للتأكد من صحتها و تصحيح ما يشوبها من أخطاء و بالمقابل إلزام الجهة القائمة على نظام المعلومات بضمان سرية المعلومات فوجود مثل هذه القواعد القانونية يعد من الضمانات الوقائية الهامة و الأساسية في حماية الحياة الخاصة للأفراد في مواجهة نظم المعلومات الشخصية كونها تضمن تجنب الاعتداء على الحق في الحياة الخاصة قبل وقوعه.

إن تناول مبدأ الطمأنينة باعتباره احد المبادئ التي يجب أن عليها نشاط نظم المعلومات الشخصية يقتضي دراسة حق الاطلاع و التصحيح و الالتزام بسرية المعلومات و هو ما سيتم تناوله في فروع ثلاث.

حق الاطلاع.

إن حق الشخص في الاطلاع[1] على ما يخصه من بيانات و معلومات تم تخزينها في ذاكرة الكمبيوتر يقتضي تناول أربع الأولى إقرار التشريعات لهذا الحق و الثانية المقصود الحق و الثالثة ما يبرر منح الشخص هذا الحق و أخيرا طرق مما هذا الحق

1- إقرار حق الشخص في الاطلاع: من البيانات الوقائية الحق في الحياة الخاصة في مواجهة نظم المعلومات الشخصية إقرار حق الشخص في الاطلاع على ما يخصه من بيانات و معلومات تم تخزينها في ذاكرة الكمبيوتر[2].

---

[1] Claudine Guerrier, Marie-Christine Monget, Droit et sécurité des télécommunications. Edition Springuer, 2000, p.245.

[2] نعيم مغبغب :مخاطر المعلوماتية والانترنت – دار النهضة العربية – القاهرة – 1998، ص249.

و نظرا لأهمية حق الاطلاع فقد أقرته غالبية الدول التي سنت تشريعات خاصة للمعلوماتية بل إن بعض الدول قد اعتبرت حق الشخص في الاطلاع من الحقوق الدستورية كالبرتغال[1] التي نص دستورها في المادة 35ف1 على حق المواطن في معرفة المعلومات التي تتعلق به و ما تتضمنه نظم المعلومات من بيانات خاصة به.

وفي نفس الاتجاه سار المشرع الفرنسي في قانون 1978 الخاص بالمعلوماتية و الحريات الذي نص على حق الشخص في الاطلاع على البيانات في المادة الثالثة منه.

وقد أكد الارشاد الأوروبي رقم 46/95 الصادر في 24 تشرين الأول 1995 على ضرورة حماية الحقوق الأساسية و حريات الأشخاص الطبيعيين و بصفة خاصة الحق في حرمة الحياة الخاصة في مجال معالجة البيانات الشخصية، وأكّد في المادة 12 على حق المواطن في الاطلاع على البيانات المتعلقة به[2].

2- المقصود بحق الاطلاع: يقصد بحق الشخص في الاطلاع على البيانات المعالجة من قبل نظم المعلومات، معرفة الشخص كل ما يتعلق به من بيانات شخصية سجلت على الكمبيوتر و مصادرها و طرق معالجتها، و كذلك مضمون المعلومات المتعلقة به بعد معالجتها.

فالحق في الاطلاع الممنوح للشخص كضمانة وقائية لحماية حياته الخاصة لا يقتصر على توفير سبل معرفته بمضمون البيانات و المعلومات التي تم تخزينها في الكمبيوتر، بل يشمل أيضا حقه في معرفة مصدرها و طرق معالجتها آليا و الأسس التي قام عليها نظام المعالجة، إن معرفة مصدر البيانات التي تم تجميعها

---

[1] مدحت رمضان: الحماية الجنائية للتجارة الالكترونية، المرجع المشار إليه سابقا، ص80.

[2] Alain Bensoussan. Internet, aspects juridiques, Paris, Hermes, 1996, p80.

و تسجيلها و تخزينها في الكمبيوتر وفقا للرأي الراجح في الفقه[1] يعد ضرورة تستلزمها حماية الحياة الخاصة للأفراد و خصوصا في نظم المعلومات التابعة لأشخاص القانون الخاص نظرا لعدم وجود أي مصلحة للجهة القائمة نظام معلومات مرتبطة بمصلحة عامة تبرر المساس بمصالح الأفراد و تستوجب عدم افشاء مصدر الحصول على المعلومات[2]، بخلاف ما هو عليه الحال في المجالات التي تقتضي المصلحة العامة فيها عدم افشاء مصدر المعلومات كما هو الحال في الصحافة و الشرطة، نظرا لاختلاف المصالح محل التعارض، فلا يكون ملزما لنظم المعلومات التابعة لها في اطلاع الشخص على مصدر المعلومات الخاصة به.

كما أن معرفة الشخص بالطرق التي ستتم المعالجة الآلية للبيانات المتعلقة به و نتائج هذه المعالجة يحمل أهمية خاصة في حالة البيانات غير الشخصية التي يترتب على معالجتها استخلاص حكم أو تقييم للشخص يحتج به الغير في مواجهته[3].

3- ما يبرر حق الشخص في الاطلاع: إن ما يوجب اعطاء الشخص الحق في الاطلاع على البيانات المتعلقة به ز التي يتم معالجتها آليا هو ما تتمتع به نظم المعلومات من امكانيات فائقة في تجميع و تخزين البيانات من مختلف المصادر من غير موافقة الشخص و دون علمه، وكذلك ما تتمتع به من امكانية نقل

---

[1] حسام الدين كامل الاهواني، الحق في احترام الحياة الخاصة ، دراسة مقارنة، دار النهضة العربية، 1978، ص49.

[2] Robert Lindon, La presse et la vie privée, J.C.P 1965, 1, 1987.

[3] Robert Badinter: Le droit au respect de la vie privée", JCP 1968, n.2136.

المعلومات المعالجة إلى مختلف إرجاء العالم[1]، في ظل انفرادها في تحديد قواعد الأمان بعيدا عن الأشخاص التي تتعلق بهم هذه المعلومات.

وإن هذا الوضع من شأنه أن يخلق عدم التوازن بين نظم المعلومات و بين الأفراد، وعدم التوازن هذا في حد ذاته يكفي لإقرار حق الاطلاع على البيانات لكل شخص تتعلق به هذه البيانات كضمان وقائي لحماية حياته الخاصة في مواجهة المخاطر المحتملة لنظم المعلومات.

4- طرق الاطلاع على البيانات: طرق ممارسة حق الاطلاع على البيانات المختزنة في نظام المعلومات نوعان، الأولى مباشرة و الثانية غير مباشرة[2].

يكون الاطلاع مباشرا إذا قام الشخص المتعلقة به البيانات بالاطلاع عليها بنفسه، أو إذا حصل على مستخرج من هذه البيانات.

و الاطلاع المباشر يقتضي أن يمارسه الشخص نفسه و لا يجوز التوكيل فيه لأنه من الحقوق الفردية التي لا يجوز ممارستها عن طريق الغير في الأصل، إلا أن ذلك لا يمنع الشخص من الاستعانة بمستشار يصحبه معه عند الاطلاع و إذا كان الشخص المتعلقة به المعلومات ناقص أو عديم الأهلية فان الممثل القانوني هو الذي يمارس نيابة عنه حق الاطلاع.

أما الاطلاع غير المباشر، فانه يحصل اذا تم الاطلاع على البيانات من قبل شخص آخر غير الشخص المتعلقة به البيانات و يكون معرفة هذا الأخير بالمعلومات عن طريق الشخص الأول الذي اطلع عليها و الاطلاع غير المباشر

---

[1] هدى حامد قشقوش: جرائم الحاسب الالكترونى فى التشريع المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992، ص145.

[2] Pierre DEPREZ et Vincent FAUCHOUX. Lois, Contrats et Usages du. Multimédia, ed. Dixit, 1997, p.123.

يكون في الأحوال التي يحظر فيها القانون على الشخص المتعلقة به المعلومات الاطلاع عليها شخصيا، و إعطاء غيره حق الاطلاع عليها نيابة عنه[1].

ومن اهم صور الاطلاع غير المباشر للبيانات و المعلومات المتعلقة بالحياة الشخصية، إعطاء الطبيب الذي يحدده المريض الحق بالاطلاع على المعلومات التي تتعلق بحالته الصحية، و حظر الاطلاع المباشر للمريض شخصيا، فيقوم الطبيب باطلاع المريض على هذه المعلومات وفقا للقواعد العامة في العلاقة بين الطبيب ووفقا لأخلاقيات مهنة الطب[2]. وهذا الأمر يحصل في الحالات التي يكون فيها المريض مصابا بمرض خطير، لا أمل من الشفاء منه رغم استخدام طرق ووسائل المعالجة الممكنة و المعروفة. و بالتالي فان هذا التساؤل لا يثار في الحالات التي لا تكون فيها حياة المريض معرضة للخطر إذ يعطي الأطباء النصائح و المعلومات مفصلة للمريض.

وهنا يثار التساؤل حول حق المريض في معرفة المعلومات الكاملة، و هل يتوجب على الطبيب إعطاؤه المعلومات كاملة؟

في الواقع لا يوجد نص قانوني صريح بهذا الخصوص، إلا الفقه قد انقسم إلى اتجاهات مختلفة في الإجابة على هذا التساؤل[3]، فالاتجاه الأول يعارض وبشكل قاطع اطلاع المريض على انعدام الأمل من شفائه كون ذلك أمرا منافيا للأخلاق

و من شأنه أن يؤدي إلى زيادة الآلام النفسية و الجسدية للمريض. أما الاتجاه الثاني فيرى إمكانية قول نصف الحقيقة أي إبلاغ المريض المريض عن حالته

---

[1] حسام الدين كامل الاهواني، الحق في احترام الحياة الخاصة، المرجع المشار إليه سابقا، ص50.

[2] نعيم مغبغب :مخاطر المعلوماتية والانترنت، المرجع المشار إليه سابقا، ص232.

[3] نعيم مغبغب :مخاطر المعلوماتية والانترنت، المرجع المشار إليه سابقا، ص247.

الخطرة إجمالا دون التصريح عن انقطاع الأمل في شفائه. أما الاتجاه الثالث نو الأخير فيرى انه لا ينبغي إلزام الطبيب في جميع الحالات بإبلاغ المريض عن انقطاع أمل شفائه، كتكتل الحالات التي تكون فيها نفسية المريض غير مستقرة و بشكل واضح، او في تلك الحالات التي لا يكون لديه إدراك سليم، أما إذا كان المريض متمتعا بوعي و بإرادة قوية و يملك عقلا سليما و هادئا، و يطالب بمعلومات دقيقة عن مرضه وعن طريق علاجه المحتملة و عن آفاق هذا العلاج، فينبغي الإقرار للمريض بحق معرفة الحقيقة[1].

و نحن نرى أن في هذه الحالة أي في حالة إصابة المريض بمرض عضال و لا أمل من شفائه فانه ينبغي النظر في دوافع المريض في معرفة المعلومات الحقيقة[2] ، عن حالته الصحية. فإذا كانت هذه الدوافع قوية وذات أهمية فلا يمنع من اطلاعه على هذه المعلومات، كما لو كان المريض يرغب في وضع وصية، أو تقديم معلومات هامة عن وقائع شهدها.

الحق في التصحيح.

من الضمانات الوقائية الأساسية والهامة لحماية الحياة الخاصة في مواجهة نظم المعلومات الشخصية، إعطاء الشخص الحق في تصحيح البيانات الخاطئة و غير الدقيقة[3]، حيث يعد هذا الحق من اهم موضوع قانون المعلومات.

---

[1] Mireille Delmas-Marty. Criminalité économique et atteintes à la dignité de la personne. Éditions de la Maison des sciences de l'homme, Paris, 1997, p.155.

[2] Philippe Rose: La criminalité informatique à l'horizon 2005- Analyse prospective, editions L'Harmattan, 1992, p.54.

[3] نعيم مغبغب :مخاطر المعلوماتية والانترنت، المرجع المشار إليه سابقا، ص250.

و إذا كان حق الشخص في التصحيح تمليه القواعد العامة في القانون، الا أن التشريعات الخاصة بالمعلوماتية عملت على تنظيم هذا الحق بصورة مفصّلة، اذا ان قانون المعلوماتية و الحريات الفرنسي في المادة 20 منه أعطى الشخص الحق في تصحيح و تكملة وز إيضاح او محو المعلومات الخاصة به اذا كانت قد تغيرت، و كذلك المعلومات التي يكون الحصول عليها أو استخدامها او الاحتفاظ مشروع قانونا[1].

ويقصد بحق التصحيح، باعتباره إحدى الضمانات الاساسية الحياة الخاصة، ان يكون للشخص من جهة أولى الامكانية في الاخطاء في البيانات الشخصية و المعلومات المعالجة آليا والمختص نظام المعلومات التي من شانها أن تولد لدى الغير فكرة مختلفة حقيقة الشخص، ومن جهة أخرى محو البيانات التي تم تخزينها غير مشروعة.

فالتصويب يكون في الحالة التي يتبين فيها للشخص بعد على البيانات المتعلقة به التي تم جمعها وتخزينها فيها بصورة مشروعة على موافقته او بناء على نص القانون، بانها غير دقيقة او انها قديمة أو غير صحيحة تبعا لمعالجة البيانات المتعلقة به فيكون له الحق في أن يطلب من الجهة القائمة على نظام المعلومات اجراء التعديل المناسب الذي يظهر حقيقة شخصيته كما هي عليه في الواقع.و يكون لزاما على الجهة القائمة على نظام المعلومات إجراء التصحيحات التي يطلبها الشخص،و إلا انعقدت مسؤوليتها القانونية.

ويكون للشخص أن يطلب محو البيانات التي تم تجميعها وتخزينها بطريقة غير مشروعة،مثل تسجيل البيانات المحظورة أو التي تم الحصول عليها بالغش و

---

[1] Bensoussan Alain, Salvator Maurice, Risques informatiques, parades techniques et juridiques, París, Editions des Parques, 1983. P.121.

التدليس.وكذلك يجوز طلب محو البيانات و المعلومات التي لا يجوز الاحتفاظ بها،و كذلك أن يطلب محو البيانات القديمة[1].

فإذا قبض على فرد بصورة مؤقتة،فيجوز له المطالبة بمحو مثل هذه وعدم إبقائها مسجلة في ملف القبض المؤقتوذلك في الحالات التالية[2]:

- إذا تبين بأن التوقيف كان مجرد حجز إحتياطي ولم يؤد إلى السجن بأدلة قضائية.
- إذا حصل التوقيغ من جراء جريمة بسيطة.
- إذا تبين بأن التوقيف لم يكن قانونيا، و إذا أعلنت المحكمة عدم قانونيته.

وتلتزم الجهة القائمة على نظام المعلومات بإجراء التصحيح من تلقاء نفسها إذا علمت بعدم صحة ما لديها من بيانات مقارنة بالمعلومات الصحيحة، وذلك دون أن يطلب التصحيح من قبل صاحب الشأن[3].

إن حق الشخص في التصحيح يعد من الضمانات الوقائية الهامة لحماية الحياة الخاصة في مواجهة نظم المعلومات وذلك لأسباب عدة ألا وهي:

أولا: إن القدرة الفائقة للكمبيوتر في جمع و تسجيل وتخزين واسترجاع قدر كبير من البيانات في وقت قصير جدا قد سهل الولوج إلى كل ما يتعلق بالحياة الخاصة لافراد بطرق مختلفة منها ما هو مشروع و منها ماهو غير مشروع، على النحو المشار إليه سابقا، إن الوصول إلى البيانات بطريق غير مشروع،

---

[1] محمد عبد المحسن المقالع: حماية الحياة الخاصة للأفراد وضمانتها في مواجهة الحاسوب الآلي، المرجع المشار إليه سابقا، ص162.

[2] Lilian edwards and charlotte waeldelaw and the internet,"Rugulating cyber space", hart publishing,
exford.1997, p.225.

[3] Alain Bensoussan. Internet, aspects juridiques, Hermes, op. cit, p107.

يمكن أن يجعل المعلومات تعتمد في جمعها و تخزينها للبيانات على و ثائق غير واضحة أو على تحريات غير دقيقة.

وهذا الأمر لا يستبعد معه وجود أخطاء من شأنها أن تعطي فكرة مخالفة عن حقيقة الشخص، مما يلحق الأذى المادي و المعنوي بالشخص.و إن تفادي مثل هذه الأضرار يعد يعد مبررا أساسيا في الشخص الحق في التصحيح كضمان وقائي لحماية حقه في الشخصية.

ثانيا: كما أن من مبررات إعطاء الشخص الحق في التصحيح أيضا الأثار الخطيرة الناتجة عن الأخطاء التقنية التي تحدث في جهاز الكمبيوتر ذات، و إختلال الضغط الكهربائي الذي يترتب عليه دمج البيانات المختلفة، وإختلال في تصنيفها و تنظيمها،أو محو تسجيلها، مما ينتج عنه نسبة معلومات معينة لشخص لا تتعلق به أصلا من شأنها إعطاء فكرة غير حقيقة عن حالته الإجتماعية أو وضعه المالي أو إنتمائه السياسي.

إن تفادي مثل هذه الأضرار قبل حصولها تكون مبررا أيضا لإعطاء الشخص الحق في التصحيح كضمان وقائي هام.

ثالثا: إن الهدف من إعطاء الشخص الحق في الإطلاع على البيانات و المعلومات المتعلقة به المختزنة في نظام العلومات يكمن -كما رأينا- في توفير قدر من طمأنينة للشخص بصحة هذه المعلومات و هذا الأمر يقضي عند إكتشاف الشخص لأخطاء فيما نسب إليه من معلومات أن يكون له حق تصحيحها أو طلب محوها[1]. فإطمئنان الشخص على ما تم تخزينه في نظام المعلومات يتفق و حقيقة

---

[1] Mireille Delmas-Marty. Criminalité économique et atteintes à la dignité de la personne. Éditions de la Maison des sciences de l'homme, Paris, 1997, p.138.

ما هو عليه في الواقع لا يتحقق فقط بالإطلاع بل بما يكون له من حق في تصحيح الأخطاء و محوها.

رابعا: إن إعطاء الشخص الحق في التصحيح يعتبر من الحقوق الملازمة للشخصية، فلكل شخص الحق في لا يأخذ الناس عنه فكرة مغايرة في حقيقة ما هو عليه و هذا الأمر يستلزم أن يكون له الحق في بيان حقيقة شخصية و أن يكون ما يطلع عليه الغير مطابق للواقع.

إن حق التصحيح باعتباره من الحقوق غير المالية للشخصية، فإن ممارسته يتوجب أن تتم من قبل الشخص نفسه يجوز أن يقوم بممارسة هذا الحق من قبل الوكيل، أما إذا كان ناقص أو عديم الأهلية فإن الولي أو الوصي هو الذي يقوم بممارسة الحق نيابة عنه، و بعد وفاة الشخص يكون لورثته الحق في ممارسة الحق و الهدف من ذلك تصحيح كل ما من شأنه الإساءة لمورثهم و الحالة الوحيدة التي يمكن لغير الشخص الكامل الأهلية هذا الحق نيابة عنه و هو على قيد الحياة هي عندما لايمون الشخص الحق في الإطلاع بصورة مباشرة على البيانات و المعلومات يمارس حق الإطلاع غيره بحكم القانون كما هو الحال بالنسبة للمريض ففي هذه الحالة يكون للطبيب الذي إختاره المريض الإطلاع المعلومات الحق في طلب تعديلها و تصويبها أو محوها.

بالإستناد لما تقدم، إن حق التصحيح يقضي وجود أخطاء البيانات أو المعلومات، ولكن السؤال الذي يمكن أن يثار هو هل يتوجب على الشخص المعني إثبات وجود الأخطاء التي تم التصحيح؟

بالعودة إلى القواعد العامة في الإثبات في هذا الخصوص بموجبها يكون عبء الإثبات على المدعي، أن يكون على المعني عبء إثبات عدم صحة البيانات و المعلومات يكون مع حرمان الشخص من ممارسة حقه في التصحيح،

و لذا ذهبت التشريعات الخاصة بالمعلوماتية إلى الخروج على القواعد العامة في الإثبات، عبء الإثبات على عاتق الجهة القائمة على نظم المعلومات، بإستثناء الحالة التي يكون الشخص نفسه الذي قدم المعلومات وذلك بهدف حماية الشخص بإعطاء حق التصحيح دفعة قوية يجعله أكثر فعالية.

وإذا ثبت حق الشخص في التصحيح فإن التصحيح يجب إبلاغه إلى الغير الذين سبق تزويدهم بالمعلومات الخاطئة أو غير الدقيقة و على الآخرين إجراء اللازم في أجهزتهم.

مبدأ الالتزام بالسرية.

لا يكفي لتوفير الطمأنينة للشخص في المحافظة على أسرار حياته الشخصية إعطائه الحق في الإطلاع على البيانات و تصحيحها، بل يتوجب أن تلتزم الجهة القائمة على نظام المعلومات بسرية البيانات والمعلومات المعالجة المختزنة في النظام[1]، و بالتالي فإن الإلتزام بالسرية من قبل الجهة القائمة على نظام المعلومات يعد من الضمانات الوقائية لحماية الحياة الخاصة في مواجهة نظم المعلومات الشخصية.

و يتحقق الإلتزام بالسرية كضمان وقائي من خلال وضع قواعد قانونية خاصة في مجال نظم المعلومات تمنع نقل أو تداول المعلومات خلافا للهدف من إقامة نظام المعلومات (كما تقدم)، وأيضا تلزم الجهة القائمة على نظام المعلومات بإتخاذ و سائل الأمان الفعالة التي تحول دون إمكانية وصول الغير إلى ما يخص الأشخاص من بيانات و هو مختزنة في النظام.

---

[1] محمد عبد المحسن المقالع: حماية الحياة الخاصة للأفراد وضمانتها في مواجهة الحاسوب الآلي، المرجع المشار إليه سابقا، ص222.

و يقصد بإجراءات الأمان مجموعة من الوسائل الفنية و الإجراءات الإدارية الضرورية لمنع وصول الغير إلى المعلومات بالأفراد. وعلى ذلك فأن إجراءات الأمان لها جانبان، أحدهما فني و الآخر إداري[1].

فالجانب الفني لإجراءات الأمان يشمل كافة الوسائل الواجب اتباعها بهدف الحيلولة دون وصول الغير إلى المعلومات المختزنة في النظام أو تسرب هذه المعلومات و إطلاع غير منيحق له الإطلاع عليها[2].

فوضع القواعد الخاصة بإلزام الجهة القائمة على المعلومات باتباع إجراءات الأمان الفنية[3]، يعد من الضمانات و لا سيما بعد ازياد مخاطر المعالجة الآلية للبيانات الشخصية و الوصول إليها من قبل غير المصرح له بالإطلاع على المعلومات بطريقة غير مشروعة[4].

ومن وسائل الأمان الفنية استخدام كلمة سرية تجعل الاختراق من قبل الغير لنظام المعلومات صعبا، وأيضا استخدام برمجيات مشفرة صعبة الاختراق، وكذلك استخدام برامج رقابة الدخول المنطقي الذي يعمل على عدم السماح لغير المخول لهم الإطلاع على المعلومات الإطلاع عليها، وكذلك استخدام البرمجيات الكشفية او التحذيرية و التي تعمل على تحديد خطرا و شيك و ومثال على ذلك البرمجيات الكشفية التي تعطي جرس إنذار عند محاولات الدخول غير المشروعة أو غير المصرح بها.

---

[1] Jean et Frayssinet Jean, Les libertés individuelles à l'épreuve des Ntic, Pul, 2001, P.45.

[2] محمد الشوابكة: جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، عمان، 2004، ص180.

[3]Claudine Guerrier, Marie-Christine Monget, Droit et sécurité des télécommunications. Edition Springuer, 2000, p.245

[4] Jean Pierre Chamoux: Menaces sur lordinateur, éd. Seuil, 1986, p.96.

والواقع ان الجانب الفني لإجراءات الأمان الواجب إتباعها من نظم المعلومات لايمكن ان يحقق حماية مطلقة للحياة الخاصة بل حماية نسبية و يعود ذلك الى تطور الوسائل التقنية للوصول الى المعلومات. فمحاولة اقتحام نظام المعلومات وان اعترضته بعض الصعوبات ليس أمرا مستحيلا بالنسبة لمن يملك الخبرة الفنية و الوسائل التقنية للقيام بذلك.

أما الجانب الإداري لإجراءات أمان المعلومات، فهو يتعلق بحسن التنظيم الإداري و الفني للجهة القائمة على نظام المعلومات وحسن اختيار الموظفين و العاملين بها، ووضع النظم اللازمة لرقابتهم من اجل المحافظة على سلامة المعلومات. ويمكن ان تكون هيئات الرقابة إما من قبل الدولة أو هيئات خاصة وهي تقوم بالحماية عن طريق: إنشاء لجان ادارية لتعقب الانتهاكات وتلقي الشكاوى وإنشاء هيئات تتولى الترخيص بإنشاء الكمبيوتر وجمع المعلومات وإنشاء هيئات تتولى وقف الترخيص أو إلغائه في حال المخالفات.

دور القضاء في رقابة المراقبة الرقمية.

في إطار الفضاء الرقمي العابر للبلدان، والذي هو أصلا بلا حدود، تم في وقت معين تفضيل مقاربة التنظيم الذاتي من جانب المجموعات المعنية، ولكنها لم تستطع استبعاد القضاة من هذه المنازعات الرقمية الجديدة، خاصة بعد قضايا أحدثت جدلا كبيرا في الرأي العام العالمي، مثل قضية بريسم PRISM أو قضية سنودن، التي سلطت الضوء على المخاطر الاقتصادية والسياسية التي ينطوي عليها معالجة البيانات الشخصية من قبل شركات الإنترنت الكبرى، وأشارت إلى الحاجة الملحة في تحسين حماية المواطنين في مواجهة تنمية وعولمة تدفق البيانات.

ولذلك فمن المهم أن نفهم كيف تتعامل العدالة مع هذا الفضاء الإلكتروني. عموما يتدخل القاضي لحل النزاعات وهي كثيرة على الإنترنت. ولذلك فإن العدالة معنية بشكل خاص بهذا الموضوع. بيد أن مشاركة القضاة تختلف باختلاف الجهة القضائية التي ينتمون إليها.

كما أشار القاضي جان جاك غوميزJean-Jacques Gomez ، وهو رائد من روّاد القضاء الرقمي، أصدر الأحكام القضائية الأولى بشأن الإنترنت، إلى أنه " قد مضى أكثر من عشرين عاما على الهيئات القضائية من العمل المتواصل في محاولة لتنظيم استخدامها مع احترام حقوق الجميع"[1].

---

[1] Marie-Anne Frison-Roche, Internet espace d'interrégulation, dalloz, mai2016, p.167.

بالفعل فإن الإنترنت تجبرنا على إعادة التفكير في الأطر التقليدية لتنظيم الأنشطة الإعلامية والمتعلقة بالشبكة القائمة على تدخل الدول وبالنتيجة إلى تدخل جهاز العدالة.

يظهر جليا إذن أن للقضاة دور المنظم في المجتمع الرقمي، ولكن تختلف أهميته بحسب ما إذا تعلق الأمر بالقاضي الدستوري أو الإداري أو الجزائي.

ولذلك سيكون من الضروري دراسة مدى قدرة القاضي على حماية الحريات الرقمية وفقا لما إذا كان ينتمي إلى القضاء الدستوري أو الاداري أو الجزائي.

وفي غياب اجتهاد قضائي في الجزائر منظم لفضاء الانترنت، كنتيجة لغياب أنظمة قانونية حديثة مواكبة لرقمنة الحياة العامة، في مجال حماية البيانات الشخصية و الحريات الرقمية على سبيل المثال لا الحصر. الأمر الذي يدفعنا إلى الرجوع ككل مرة إلى التجربة الفرنسية والدولية.

وفي الواقع فإن للقاضي الدستوري دور أساسي حيث يصادق على الأحكام التشريعية بينما يسهر القاضي الاداري و الهيئات الادارية المستقلة على مدى احترامها، في حين أن القاضي الجزائي له دور منظم في الوقت المحدد لا يمكن تجنبه، فإن الممارسة القضائية الحالية في الولايات المتحدة الأمريكية، وفي أوروبا ولا سيما محكمة العدل التابعة للاتحاد الأوروبي، تبين أن لهذه الهيئات دورا متناميا في حماية الحريّات الرقمية.

دور القاضي الدستوري والإداري والهيئات الادارية المستقلة في حماية الحريات الرقمية.

ويستمد القاضي الدستوري شرعية سلطته من الرقابة التي يمارسها على النصوص التشريعية والتنظيمية، وإن هذه القوانين لا سيما عندما يتعلق الأمر

بتنظيم شبكة الإنترنت تخضع بشكل متزايد لإشراف القاضي الدستوري الفرنسي الذي يقوم تدريجيا ببناء اجتهاد قضائي متعلق بتنظيم الإنترنت بهدف حماية الحريات العامة.

بينما يسهر القاضي الاداري و الهيئات الادارية المستقلة في ظل القوانين التي تهدف إلى محاربة الارهاب والتي كثفت من عمليات المراقبة الرقمية، على ممارسة الرقابة على أعمال الادارة ومدى احترامها لمبدأ الشرعية **(فرع ثاني)**.

دور القاضي الدستوري في حماية الحريات الرقمية.

يجب أن تكون الإنترنت فضاءا لممارسة الحريات، وليس فضاءا خارج القانون. أو بعبارة أخرى مكان للتعبير عن الحريات الأساسية وممارستها في إطار احترام المتطلبات الدستورية. من خلال هذا الحوار تتبلور الرؤية الجماعية التي يمكن أن تكون لدينا عن البشرية في العالم الرقمي.

وفي هذا السياق حدث التقارب بين الإنترنت والدستور في تأكيد الحريات الرئيسية المكفولة دستوريا **(أولا)** وأيضا في تحديد التوازنات الكبرى بين الحريات في مواجهة المخاطر الجديدة للإنترنت **(ثانيا)**.

أولا: التكريس الدستوري للحريات الرقمية.

منذ البداية أو تقريبا ومن خلال الآباء المؤسسين، اعتبرت الإنترنت فضاءا اجتماعيا، تيرا نوفا أو يوتوبيا أعلنت استقلالها عن حكومات العالم[1]. في الواقع فإن الأمور أقل وضوحا وبصرف النظر عن مثالية المؤسسين، فإن تعمير هذا

[1] Electronic Frontier Foundation, « A Declaration of the Independence of Cyberspace », John Perry Barlow (1996):
https://projects.eff.org/~barlow/Declaration-Final.html

الفضاء من طرف الجمهور العريض هو الذي يؤدي إلى تأكيد الحريات الدستورية على شبكة الإنترنت.

1- الاعتراف بفضاء جديد لحرية التعبير.

لم تناقش مسألة حرية التعبير على الانترنت في الجزائر والدول العربية بمزيد من الاهتمام الذي ناله عالميا بحيث لم يتم تكريسها دستوريا ولا قضائيا.

وعلى خلاف ذلك فإن المستجدات الرئيسية التي جاء بها قرار المجلس الدستوري الفرنسي الصادر في 10 جوان 2009[1]، والذي يعتبر بلا شك "حجر الزاوية" في القانون الدستوري الرقمي، تكمن بالتأكيد في تكريس وصول المواطنين إلى شبكة الإنترنت باعتبارها شكلا من أشكال تطبيق المادة 11 من إعلان حقوق الإنسان والمواطن لعام 1789، وهذا يعني ليس فقط تكريسا لحق دستوري، ولكن أيضا كما شدّد على ذلك المجلس على " واحدة من أغلى حقوق الإنســـــان، فكل مواطن يستطيع إذا: الكلام، الكتابة، الطباعة بحرية، إلا في حالات إساءة استعمال هذه الحرية المحددة في القانون".

ومع ذلك، فإن حكمة المجلس لم تذهب إلى حد الاعتراف بـــ "حق الوصول إلى الشبكة" كحق دستوري كان من شأنه أن يؤدي إلى "ضمان حق عام ومطلق للجميع". يمكننا أن نقرأ بالتأكيد سياسة المجلس على المضي قدما في دفاعه عن الحريات الأساسية المواكبة للعصر ولأدواته دون الدخول في التفاصيل التقنية في مجال جديد ومتغير.

في عصر الادارة الإلكترونية والشبكات الاجتماعية، أصبحت شبكة الإنترنت في كثير من الأحيان وسيلة لضمان المرفق العام – واستمراريته. وهو ما يعبر

---

[1] Décision no 2009-580 DC du 10 juin 2009: Loi no 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet (non-conformité partielle): *JORF* du 13 juin 2009, p. 9675.

عنه التحول الالكتروني التدريجي لبعض الإجراءات الإدارية. وتشكل أيضا عنصرا أساسيا في العلاقات الاجتماعية، ومكان لممارسة الحقوق الأساسية. وهي عموما فضاء جديد للمعلومات والآراء.

وحتى إن لم يعترف المجلس الدستوري بحق إيجابي في الوصول إلى شبكة الانترنت، ليس من المستبعد أن مثل هذا التكريس قد يأتي في نهاية المطاف إلى تعزيز أهمية الإنترنت في "الحياة الديمقراطية"، وبهذا الاعتراف تبرير التوفيق بينه وبين الحقوق والحريات الأساسية الأخرى، مثل حرمة الحياة الخاصة.

2- الاعتراف الدستوري بالحق في حماية البيانات الشخصية.

إن ممارسة الحريات العامة على الإنترنت لا يمكن فصله عن مسألة حماية حرمة الحياة الخاصة. ومع ذلك فإنها تساهم بشكل أساسي في تجديد مفهومها.

يتعرض كل فرد اليوم لتعقب مزدوج في المكان والزمان. في المكان، ويرجع ذلك إلى الانتشار المتزايد لأنظمة المراقبة بالفيديو، والأنظمة البيومترية وأنظمة تحديد الموقع الجغرافي، مما يشكل تحديا لحرية التنقل. ولكن أيضا في الزمان، من خلال التنميط والاستهداف التي تسمح به محركات البحث، والشبكات الاجتماعية التي تؤدي إلى خلق ذاكرة مطلقة وعامة عن الآراء والسلوكيات الفردية.

أما في المسائل الدستورية، فإن الاعتراف بمبدأ احترام الحياة الخاصة من جانب المجلس الدستوري[1] قد تم حتى الآن تصوره أساسا من منظور "دفاعي". والهدف من ذلك هو التأكد من تناسب التدابير التي يحتمل أن تؤدي إلى المساس به، وعلى وجه الخصوص تقيّد القواعد المتعلقة بتحديد هوية الأفراد بالأهداف ذات القيمة الدستورية مثل النظام العام والأمن والدفاع عن حق الملكية. ويرتبط

---

[1] Isabelle Falque-Pierrotin, la constitution et l'internet, Dalloz « Les Nouveaux Cahiers du Conseil constitutionnel », 2012/3 N° 36, pages 35.

تحديد هوية الأفراد في المقام الأول بالالتزامات المفروضة على مقدمي خدمة الإنترنت بالاحتفاظ بالبيانات الناشئة عن أنظمتهم، وإن قضية الوصول[1] إلى هذه البيانات تشكل الجزء الأكبر من المنازعات الدستورية.

ومع ذلك فإن حماية البيانات الشخصية التي تنبثق من حماية حرمة الحياة الخاصة، والمكرّسة دستوريا تشكل اليوم مفهوما جديدا.

ويبدو أن احترام حرمة الحياة الخاصة لم يعد يشمل مسألة حماية البيانات الشخصية برمتها. والواقع أنها أصبحت تشكل حقا أساسيا مستقلا بذاته، عند مفترق الطرق بين حق الملكية- البيانات التي ينشرها الشخص على شبكة اجتماعية، هل هي ملك له؟، وحرية التعبير- لاسيما عن طريق المدونات- وحماية حرمة الحياة الخاصة. وبصورة أعم فإن إثارة مسألة حرمة الحياة الخاصة على الإنترنت، يطرح اشكال البيانات الشخصية التي يمكن أن تتاح بمبادرة من مالكها أو بدون معرفته، والتي قد تكون محل إعادة استخدام أو استغلال أو تخزين يؤدي إلى الحاق الضرر بالأشخاص.

ويطرح أيضا إشكال آخر يتعلق بتفكك وحدة الفرد في سحابة بيانات تمثله جزئيا ولكن اعادة تشكيلها يؤدي إلى المعرفة الوثيقة بما في عقله وجسمه. ويكفي أن ننظر إلى تنوع وحجم البيانات الموجودة لنفهم أهمية مهمة الضبط التي تضطلع بها في فرنسا اللجنة الوطنية للمعلوماتية والحريات CNIL بينما تبقى هذه المهمة مفقودة في الجزائر تمارس بصفة عرضية وظرفية من طرف وزارة البريد

---

[1] V. not. Décision 2009-580 DC, précit., et Décision no 2009-590 DC du 22 octobre 2009: Loi no 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet: *JORF* du 29 octobre 2009, p. 18292, Considérant no 11, et Décision no 2011-625 DC du jeudi 10 mars 2011: Loi d'orientation et de programmation pour la performance de la sécurité intérieure: *JORF* du 15 mars 2011, p. 4630.

والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة. أصبحنا اليوم لا نعرف ككيان إنساني مستقر ولكن من خلال البيانات السلوكية، والبيومترية، والمتعلقة بالهوية المدنية، والصحة... البيانات التي نقدمها أو نتركها هنا أو هناك.

وفي هذا السياق فإنه من الضروري إعطاء الفرد إمكانية استعادة السيطرة على هذا التشتت لبياناته وتعزيز الصلة بين الفرد وتوأمه الرقمي. ولهذا لم تعد الرؤية الدفاعية الوحيدة لحماية البيانات الشخصية كافية ؛ يجب أن تكون مصحوبة بأداة أكثر إيجابية.

إن النقاش حول الحق في النسيان يشكل أول مثال في هذا الاتجاه: كل واحد منا يريد استعادة السيطرة على ما يقول على الانترنت، بما في ذلك مواقفه التي اتخذها في لحظة معينة في حياته وقد عبّر جبران خليل جبران عن النسيان في كتابه "رمل وزبد"[1] على أنه شكل من أشكال الحرّية.

ولذلك فإن الاجتهاد الدستوري في مجال الإنترنت بنّاء وفي تطور، ويأخذ في الاعتبار آثار ظهور الإنترنت على الحقوق والحريات الأساسية.

ثانيا: احترام النظام العام على الانترنت.

تواجه الإنترنت إذن مسألة الرقابة على المحتوى. وفي جميع الحالات التي يتدخل فيها المشرع، والتي تكون مرتبطة أساسا بالبحث عن شكل من أشكال التوازن، ينطوي على مواجهة بين القواعد التي تميّز شبكة الإنترنت مع الظابط القانوني الأسمى.

ومن ثم ومن خلال الرقابة النسبية التي يقوم بها المجلس الدستوري في تحديد هذا التوازن الصحيح. يواجه النظام العام حرية التعبير وهي الحرية الأولى على الإنترنت وجل المنازعات تتعلق بها.

---

[1] جبران خليل جبران، رمل وزبد، ترجمة: ثروت عكاشة الطبعة السادسة دار الشروق، القاهرة– مصر 1999.

إن موضوع احترام النظام العام على الانترنت[1] من المواضيع الأكثر جدلا في عالم الإنترنت، الأكثر تنظيما لمجال الحريات، يسعى القاضي الدستوري من خلاله إلى التوفيق بين مختلف الحقوق والحريّات الدستورية.

لقد تم قبول شكل معين من التصفية بهدف تحقيق هذا التوازن مقابل مجموعة من الضمانات المقدمة. وإن النظام الذي يقترحه القانون يتمثل في السماح للسلطة الإدارية بإخطار مقدمي خدمة الإنترنت مباشرة بعناوين المواقع ذات الصلة بالمواد الإباحية المتعلقة بالاستغلال الجنسي للأطفال. وبناء على هذا الإخطار يقوم مقدمو الخدمة بمنع وصول مشتركيهم إلى هذه المواقع. ومع ذلك يجوز الطعن في قرار السلطة الإدارية في أي وقت من قبل أي شخص معني أمام المحكمة المختصة، وعند الاقتضاء من خلال رفع دعوى استعجالية. وقد أقّر المجلس الدستوري هذه الآلية، مشيرا إلى أن "هذه القواعد تضمن التوفيق بين هدف ذي قيمة دستورية وهو الحفاظ على النظام العام وبين حرية الاتصال التي تكفلها المادة 11 من إعلان حقوق الإنسان والمواطن لعام 1789"[2].

في حين أصبحت شبكة الإنترنت مجتمعا مستقلا بذاته، و"ألاغورا"[3] رقمي جديد ومساحة للتعبير والنشر فريدة من نوعها، يحتل الاجتهاد الدستوري دورا كبيرا في الإشراف على هذه الوظائف ويؤدي وظيفة تهدئة. دون إطفاء النزاع تماما حول التصفية و الرقابة التي تسببها، أدى الحوار بين المشرع و القاضي

---

[1] Isabelle Falque-Pierrotin, la constitution et l'internet, Dalloz « Les Nouveaux Cahiers du Conseil constitutionnel », 2012/3 N° 36, pages 38.

[2] Décision 2011-625 DC du 10 mars 2011, *JORF* du 15 mars 2011, p. 4630, texte no 3, considérant no 8.

[3] أجورا (Agora) هي ساحة دائرية كان المزارعون بأثينا يلتقون بها منذ عام 406 ق.م و لكنها لم تكن حكرا عليهم بل كانت موضع التقاء الفلاسفة أيضا.

الدستوري إلى تقليل الخلافات بشكل لافت يخدم التوازن الرامي إلى حماية الحريات.

دور القاضي الإداري والهيئات الادارية المستقلة في حماية الحريات الرقمية.

إن الانترنت كنافذة دخول للبيانات والمعلومات من جميع المصادر إلى التراب الوطني، والتي يُنظر فيها إلى مراقبة السلطات العمومية بشكل سيئ، بالاضافة إلى صعوبة تحقيقها تقنيا، تسمح الإنترنت لمتدخلين خارج الاقليم الوطني وبصفات مختلفة بالتدخل في شؤون الدولة. وبهذه الطريقة كثيرا ما يمكن احباط جهود الدولة في السيطرة على نظامها القانوني **(أولا)**.

تمس تقنيات الاستخبارات بطبيعة الحال بالحريّات العامة ومكوناتها، لذا يجب أن تكون محاطة بمجموعة من الضمانات قد سبق ذكرها، مثل الهدف الذي وضعت من أجله أو تحديد مدة حفظ البيانات. ينص القانون الفرنسي على إنشاء سلطة ادارية مستقلة جديدة، كان من المفترض أن تراقب أعمال رئيس الوزراء القبلية. كما أنه ينص على اختصاص مجلس الدولة في الطعون المقدمة في في أول و آخر درجة، رغم أن معظم الفقه نادى بالاختصاص الحصري للسلطة القضائية **(ثانيا)**.

أولا: عجز السلطة العامة أمام ظاهرة الإنترنت.

تفرض الإنترنت نهجا شبكيا تفاعليا ومتعدد التخصصات القانونية، كسرا لمنطق الهرمية و الانغلاقية، يفرض على الدول المتعودة على أنظمة قانونية

وآليات تنظيمية عابرة للحدود، التكيف مع عصر "تفاعل المعايير"[1]. ويتعين عليها بالفعل تكييف أجزاء معينة من تشريعاتها والاعتماد على الآليات التنظيمية التي تتطلب تدخل هيئات دولية وخبراء وجهات فاعلة خاصة في مجالات عديدة. تواجه الدولة أيضا في المجال الدستوري صعوبة التوفيق بين الامتيازات الكلاسيكية للسلطة العامة مع آثار معينة للثورة الرقمية. أولا لأن الشؤون الداخلية للدولة لم تعد كذلك: ففي جميع الميادين، فيما يخص التوجهات السياسية للدول، وقرارات قادتها أو قضاتها، ومحتوى نصوصها الأساسية، وتطور ممارساتها المؤسساتية، يتم التشكيك في كل ما سبق على الانترنت، تحت نظر "المجتمع الدولي". وباسم حرية التعبير والديمقراطية يمكن أن تنتقد قرارات المحاكم[2]، وأن تشجع الأهداف االانفصالية لبعض المقاطعات(دعم استقلال التبت، أو كيبيك، أو كوسوفو)، وأن تناقش قرارات المسؤولين السياسيين(قرارات العفو التي أصدرها ملك المغرب في أوت 2013)، وأن تكذّب الخطابات الرسمية (كالكشف عن "كواليس" الألعاب الأولمبية في بكين أو عن الأسباب الواهية لحرب العراق).

ثانيا وبصفة خاصة بسبب تطور الإنترنت هناك صعوبة متزايدة على الدول في فرض خيارات سياسية معينة أو قرارات معينة تتخذها السلطات العمومية على أراضيها. يمكن أيضا أن تعجز السلطة العامة، وأن تنتهك قوانينها وأن تهدّد

---

[1] Voir, sur ce concept, les travaux de Marie-charlotte Roques-Bonnet, Le droit peut-il ignorer la révolution numérique ?, Michalon, 2010, p. 332 ; N. Sautereau, « Internet et le droit global: approche critique », L'observateur des Nations unies, 2011-2, vol. 31, p. 61.

[2] Voir les commentaires sur divers blogs et sites web concernant la décision du Conseil constitutionnel sénégalais du 27 janvier 2012 validant la candidature du président sortant Abdoulaye Wade et invalidant celle du chanteur Youssou Ndour, celui-ci ayant appelé la Communauté internationale a manifester sa désapprobation.

مصالحها بسبب التستر، والطابع العابر للحدود، والمتقلب الذي تتسم به هذه الوسيلة الاعلامية الجديدة.

لمرفق القضاء علاقات متعددة بموضوع الثورة الرقمية. فإذا نظرنا له باعتباره مرفق من المرافق العامة، فإنه مخاطب بموضوع الحكومة الرقمية. وبالتأكيد فإن استخدام مرفق القضاء لتكنولوجيا المعلوماتية والاتصالات يقدم خدمة كبيرة للمتقاضين والمتعاملين مع مرفق القضاء. وتحقيق الهدف السابق يقتضي بعض التعديلات القانونية في نظم التبليغ وكثيرا من الجهد في إعداد الموارد البشرية. وعلاقة القضاء بموضوع الحكومة الرقمية لا تقف عند هذا الحد، فكما أسلفنا فإن القضاء بشكل عام والقضاء الإداري بشكل خاص يستطيع من خلال تفسير القواعد القانونية، بمناسبة الحكم في منازعة محددة، أن يسد النقص في كثير من المجالات القانونية. ومما يساعد القاضي الإداري في النهوض بهذا العبء، المبادئ القانونية الحاكمة للمرفق العام والتي أسّسها رولاند في 1934، فمبدأ قابلية المرفق للتحول ومبدأ وجوب استمرارية سير المرافق العامة بانتظام واضطراد ومبدأ المساواة بالاضافة إلى مبدأ المشروعية تشكل قاعدة صلبة ينطلق منها القاضي الإداري وهو بصدد التعامل مع موضوع المراقبة الرقمية حماية للحريات العامة.

ثانيا: الرقابة على أعمال الادارة و كيفية حمايتها للحريات الرقمية.

يتمثل الغرض من الاستخبارات على وجه الخصوص في الحفاظ على النظام العام، ولذلك فهي تقع ضمن نطاق الظبط الإداري، وبالتالي فإن القاضي الإداري مختص.

جعل المشرع الفرنسي من رأي اللجنة الوطنية لمراقبة تقنيات الاستخبارات (التي تتألف من عضوين من الجمعية الوطنية، عضوين من مجلس الشيوخ،

قاضيان من مجلس الدولة، قاضيان من محكمة النقض وشخصية مؤهلة في مجال الاتصالات الإلكترونية) ضمانا لتنفيذ هذه التقنيات. لكن هذا الرأي المسبق يبقى استشاريا. هذه المسألة تطرق إليها المجلس الدستوري الفرنسي بمناسبة اخطاره من طرف رئيس مجلس الشيوخ بالقانون المتعلق بالاستخبارات[1] والذي أجاب بأن " إذن الوزير الأول في حد ذاته بعد أخذ الرأي اللجنة الوطنية لمراقبة تقنيات الاستخبارات لا يمس بالحق في حرمة الحياة الخاصة، ولا بحرمة المنزل أو سرية المراسلات "(الحيثية رقم 19). وبطبيعة الحال أجاب المدافعون عن هذا القانون أن المادة الجديدة 1-4-311 .L من قانون العدالة الإدارية تمنح لمجلس الدولة الاختصاص في أول وآخر درجة للنظر في الدعاوى المتعلقة باستعمال تقنيات الاستخبارات. وبالإضافة إلى ذلك يمكن إخطار مجلس الدولة من طرف أي شخص يرغب في التحقق فيما إذا كان محل مراقبة غير شرعية، وكذلك من طرف اللجنة الوطنية لمراقبة تقنيات الاستخبارات إذا رأت أن توصياتها لم تُأخذ بعين الاعتبار أو أن الإجراءات المتخذة بشأنها كانت غير كافية.

ولا شك أن حجة الضمانة القضائية اللاحقة مقبولة قانونيا ولكن معقدة للغاية من الناحية الاستراتيجية. على افتراض أن حجة الغاية من تبني هذا القانون تسمو على تلك المتعلقة بمدى التعدي على الحريات، فإن الطابع الاختياري فقط لرأي اللجنة الوطنية لمراقبة تقنيات الاستخبارات من الصعب تقبله. وبعيدا عن منطق وتجانس القانون، فإن هذا النظام يلقي بشكوك قوية ومشروعة على قانون الأمن

---

[1] Le Conseil constitutionnel a été saisi, le 25 juin 2015, sous le numéro 2015-713 DC, par le président du Sénat, dans les conditions prévues à l'article 61, deuxième alinéa, de la Constitution, de la loi relative au renseignement

الداخلي، حيث أنه للوزير الأول الكلمة الحاسمة. فوفقا للمادة L. 821-1[1] منه، يخضع استخدام تقنيات جمع المعلومات الاستخبارية إلى الإذن المسبق من الوزير الأول، الذي يصدره بعد أخذ رأي السلطة الادارية المستقلة. وإن رأيها السلبي يجب أن يكون مبررا ولكن لا يرتب أي آثار قانونية على إصدار الإذن. وفي المقابل يجوز لللجنة أن تقدم توصيات وتخطر مجلس الدولة.

وعلاوة على ذلك، ينص القانون على أنه يمكن للوزير الأول أن لا يطلب رأي اللجنة "في حالة الاستعجال المطلق" (المادة L. 821-5) - لا ينبغي الخلط بينها وبين "حالة الاستعجال العملية" التي نصت عليها المادة L. 821-6. تمارس اجراءات الاستعجال المطلق تحت رقابة مجلس الدولة، ويتم مع ذلك إعلام اللجنة الوطنية لمراقبة تقنيات الاستخبارات، و يكون الغرض منها: " لمنع المساس الخطير بالنظام العام" ولا يمكن أن تتعلق بالجمع الآني للبيانات على شبكات متعاملي الاتصالات وخوارزميات التنقيب عن البيانات المثيرة للجدل. هذه الشروط مكّنت المجلس الدستوري من عدم ابطال هذا الإجراء، بعد اخطاره من طرف مجموعة من البرلمانيين. أما بالنسبة لحالة الاستعجال العملية، ينطبق هذا الإجراء في حالة وجود "تهديد وشيك" أو "خطر كبير جدا لا يمكن معه التدخل في وقت لاحق"، وإن هذه الاجراءات أكثر تقييدا من إجراءات الاستعجال المطلق، بحيث أنها لا تتطلب إذن الوزير الأول. ومن الغريب في الأمر أن اخطار المجلس الدستوري لم يتم من طرف النواب وإنما من طرف رئيس الجمهورية[2]

---

[1] LOI n° 2015-912 du 24 juillet 2015 relative au renseignement.

[2] "Le président de la République qui a saisi le Conseil dès le 25 juin 2015, ce qui constitue une première dans l'histoire des saisines du Conseil constitutionnel s'agissant au moins des lois ordinaires". Michel Verpeaux, La loi sur le renseignement, entre sécurité et libertés, la semaine juridique - édition générale - n° 38 - 14 septembre 2015, p.1639

وأنه من المنطقي في الأخير قيام المجلس بابطاله. لخلوه من أي ضمانات إجرائية، لإعطاء صلاحيات واسعة لأجهزة المخابرات، وخاصة بوضع أجهزة للتنصت على المكالمات الهاتفية والبيانات التي تمر من خلال الهواتف المحمولة IMSIcatchers، والتي تُعد "مساسا خطيرا بالحق في حرمة الحياة الخاصة وسرية المراسلات "(الحيثية 29)[1].

دور القاضي الجزائي في حماية الحريات الرقمية.

تعتبر الجريمة الالكترونية الآن هي أكبر تحدي يواجه رجال القانون والتشريع ليس في الجزائر فقط ولكن في العالم اجمع، نظرًا لان تلك الجريمة مرتبطة بالتطور التكنولوجي الهائل الذي تشهده المعلوماتية في الآونة الأخيرة كذلك المجرم المعلوماتي الذي يختلف عن المجرم الطبيعي من حيث قدرات الذكاء والإحتيال التي تتطلب قدرات موازية ومماثلة لدى القائمين على وضع القوانين والتشريعات الخاصة بمكافحة الجريمة الالكترونية ومعاقبة مرتكبيها (فرع أول).

نتناول في مرحلة ثانية نظرة تحليلية حول حجية الدليل الرقمي أمام القضاء الجزائري، من حيث كونه دليل إثبات قائم بذاته وكيفية تبني القوانين الجزائرية المنظمة لحرية الاتصالات والمعلومات وما يتوافق مع حقيقة وجود الدليل الرقمي واعتماده كدليل إثبات جزائي شأنه شأن كافة أدلة الإثبات المتعارف عليها من شهادة الشهود والقرائن والبينة والاعتراف والدليل الكتابي وغيرها (فرع ثاني).

---

[1] Wanda Mastor, Professeur de droit public à l'université Toulouse Capitole, IRDEIC-Centre d'excellence Jean Monnet, La loi sur le renseignement du 24 juillet 2015 « La France, Etat de surveillance » ? AJDA 2015 p.2018.

حماية البيانات الرقمية في مواجهة الجريمة المعلوماتية.

يعتبر الخطر حدثا احتماليا ضارا يعتمد على الصدفة وهو مفهوم جوهري في القانون المعاصر[1]، ويتعلق بصفة خاصة بالبيانات الشخصية، التي لها قيمة مالية ولكنها أيضا مستهدفة أيضا لأغراض تجارية ولكن أيضا لأغراض قد تكون خبيثة. وقد أدى تطور الإنترنت إلى زيادة كبيرة في تداول البيانات الشخصية. بالفعل فمع تدويل المعاملات وإضفاء الطابع غير المادي عليها، أصبحت الرهانات المرتبطة بحماية البيانات الشخصية كبيرة عندما تكون في الفضاء الرقمي[2]. وتحمي البيانات الشخصية نظم قانونية مختلفة، ولكن الآراء متباينة في كثير من الأحيان بشأن مستوى الأمن الذي يجب منحه لها الذي يأثر لا محالة على قرارات الجهات القضائية في هذا المجال. ويشهد على ذلك موقف محكمة العدل الأوروبية التي ألغت في حكم صدر مؤخرا في 06 أكتوبر 2015[3] ما يسمى بنظام "Safe Harbor " بشأن نقل بيانات الأوروبيين إلى الولايات المتحدة باعتبار أن نظامها ذو حماية غير كافية.

ويجب أن نتذكر أن هذا القرار جاء في إطار وأيضا كردة فعل على قضية "Snowden" التي أظهرت للعالم أن الدولة يمكن أن تتحول إلى مراقب يسيطر على البيانات الشخصية للأفراد[4].

---

[1] Valérie Lasserre, « Le risque », Recueil Dalloz 2011, p. 1632.

[2] Myriam Quéméner, Criminalité économique et financière à l'ère numérique, Economica 2015.

[3] CJUE, 6 oct. 2015, Aff. C-362/14, Myriam Quéméner, « La fin du Safe Harbor au nom de la protection des
données personnelles: enjeux et perspectives », RLDI 2015, 120.

[4] Myriam QUÉMÉNER, Les données personnelles à l'ère numérique Quelle protection sur le plan pénal ? Revue

ما هي الردود الجزائية اليوم في مواجهة هذه المخاطر؟ وكما أشار Christian Paul في تقريره الرائد في عام 2000[1]، فإن " الإنترنت ليست في حد ذاتها فراغا قانونيا ". وهي لا تشكك في أسس القانون ". ومن ناحية أخرى من الواضح أن الإنترنت تسبب للقانون مشاكل جديدة ومتعددة.

وقد سبق وأن تطرقنا إلى المخاطر المرتبطة بإساءة استخدام الانترنت، من جرائم موجهة مباشرة ضد البيانات الشخصية وجرائم المعلوماتية و جرائم كلاسيكية سبق وأن نص عليها قانون العقوبات.

ولما أصبحت الجريمة الالكترونية واقعًا ملموسًا تواجهه الجزائر الآن، في ظل قصور تشريعي واضح في مواجهة تلك الجرائم، فإنه من الضروري التعرف على ماهية الجريمة الالكترونية.

ذهب الفقيه (Marwe) إلى أن الجريمة الالكترونية هي فعل غير مشروع يتورط في ارتكابه الحاسب الآلي – أو هو الفعل الإجرامي الذي يُستخدم في اقترافه الحاسب الآلي كأداة رئيسية، فيما عرفها الفقيه (Blat ros) بأنها كل نشاط غير مشروع موجة لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقه .وعرفها كلاوس تايدومان بأنها كافة أشكال السلوك غير المشروع الذي يُرتكب باسم الحاسب الآلي .ويرى البعض أن تعريف كلا من (Marwe) و (Blat ros)[2] مقصورين على الإحاطة بأوجه الظاهرة الإجرامية أما تعريف كلاوس تايدومان فيؤخذ عليه أنه بالغ في العمومية

---

du droit public - 01/01/2016 - n° 1 - page 71

[1] C. Paul, Les droits et libertés sur l'Internet, rapport au Premier Ministre [mai 2000], La documentation Française, 2001.

[2] د. عبد العال الديربى: الجريمة المعلوماتية – تعريفها – أسبابها وخصائصها، 13 يناير 2013 ,منشور على الموقع التالي www.acconline.com/article.detail.aspr?id:7509.

والاتساع ؛ لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع .ويدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة، تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورًا رئيسيًا.

ذهب الفقيهان (Credo & Michel) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته .وذهب رأى أخر من الفقة إلى تعريف الجريمة الالكترونية بأنها عمل أو امتناع يأتيه الإنسان، إضرارًا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب .ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر.

لاشك أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع فضلًا عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التي تختلف تمامًا عن الخصائص التي تتمتع بها الجرائم التقليدية، كما أن الجاني الالكتروني (أو المجرم الالكتروني) يختلف أيضا عن المجرم العادي.

ويــأتي فــي مقدمة أسباب الجريمة المعلوماتيــة، غاية التعلم والتي تتمثــل في استخدام الكمبيــوتر والإمكانيــات المستحدثة لــنظم المعلومــات وهنــاك أمل الربح وروح الكسب التي كثيرًا ما تــدفع إلــى التعــدي علــى نظــم المعلومات بالإضــافة إلــى الدوافع الشخصــية والمــؤثرات الخارجيــة التــي قــد تكون سبباً في ارتكــاب الجريمــة المعلوماتية.

يشير الأستاذ ليفي مؤلف كتاب "الهاكرز أبطال ثورة الكمبيوتر"[1] إلــى أخلاقيــات هــؤلاء القراصنة والتي ترتكز على مبدأين أساسيين : أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم . وأن جمع المعلومات يجب أن تكون غير خاضعة للقيود .وبنــاء علــى هــذين المبــدأين فــإن أجهــزة الكمبيوتر المعنية ما هي إلا آلات للبحــث، والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات .ومن وجهة نظر هؤلاء القراصنة فإن جميــع المعلومــات المفيــدة بوجــه عــام يجــب أن تكون غير خاضعة للقيود وبعبارة أخرى أن تتاح حرية نسخها وجعلهــا تتناسب مــع استخدامات الأشخاص. ويــرى هــؤلاء القراصنة إغلاق بعض نظــم المعلومات وعدم الســماح بالوصول إلى بعض المعلومات وخاصة بعض المعلومات السرية التي تخص الأفراد .ويعلق قراصنة الأنظمة أنهم يرغبون في الوصول إلى مصادر المعلومات والحاسبات الإلكترونية والشبكات بغرض التعلم .وقد لاحظ كل من "ليفي" و "لاندريس" أن قراصنة الأنظمة لديهم الاهتمام الشــديد بأجهزة الكمبيوتر وبالتعلم ويدخل العديد منهم في أجهزة الكمبيوتر على أنهم محترفين ويختار بعــض القراصنة الأنظمــة لتعلم المزيد عن كيفية عمل الأنظمة[2].

---

[1] Hackers: Heroes of the Computer Revolution. Front Cover. Steven Levy. Anchor Press/Doubleday, 1984 - Computer hackers - 458 pages.

[2] د. عبد العال الديربى: الجريمة المعلوماتية – تعريفها – أسبابها وخصائصها، 13 يناير 2013 ,منشور على الموقع التالي www.acconline.com/article.detail.aspr?id:7509

أصبحت الجريمة الإلكترونية موضوعا واسعا، ورغم صعوبة إيجاد تعريفا جامعا مانعا لها إلا أن اجتهاد كل من الفقهاء و الباحثين أدى إلى عدة تعريفات لها وإن كانت قد تباينت تبعا لمحل اهتمام كل فئة، فمنهم من عرفها من الجانب التقني الفني والبعض الآخر من الجانب القانوني،و من أجل مفهوم شامل للجريمة لا بد من بيان أركانها (أولا) وتحديد موقف المشرع الجزائري منها (ثانيا).

أولا: أركان الجريمة الإلكترونية.

تتمثل أركان الجريمة الإلكترونية مثل الجريمة العادية في الركن الشرعي و المادي والمعنوي:

1- الركن الشرعي :

معناه إعتراف المشرع والنص على تجريم الفعل المرتكب، "لاجريمة ولا عقوبة إلا بنص"... بالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بالجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات[1].

2- الركن المادي:

يتكون الركن المادي للجريمة الالكترونية من السلوك الاجرامي و النتيجة و العلاقة السببية،علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها، (مثلا: انشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة الا أنه لا مناص من معاقبة الفاعل).

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل ايجابي مرتكب،(مثلا: جريمة الغش المعلوماتي: الركن المادي فيها هو تغيير الحقيقة في التسجيلات الكترونية أو المحررات الإلكترونية[2].

---

[1] القانون رقم04-15 المؤرخ في10 نوفمبر2004، المادة394 مـ رر.

[2] القانون رقم04-15 المؤرخ في10 نوفمبر2004، المادة 394 مـ رر.

3- الركن المعنوي :يتكون الركن المعنوي للجريمة الإلكترونية من عنصريها أي العلم و ارادة.

ثانيا :موقف المشرع الجزائري من الجريمة الإلكترونية.

حاول المشرع الجزائري، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الإلكترونية، ويعود أسباب الاهتمام بتنظيم جرائم الانترنت من جهة تطور تكنولوجيا الإعلام أدى إلى اتساع نطاق الجريمة الإلكترونية فهي أصبحت لا تقتصر على جريمة واحدة وإنما إتسعت إلى عدة جرائم ترتكب عن طريق الهاتف وعن طريق الكمبيوتر،ولا ترتكب هذه الجريمة من طرف شخص طبيعي فقط بل تعدت إلى الشخص المعنوي ومن جهة أخرى كون القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الالكترونية الحديثة ضيف إلى ذلك المحافظة على مبدأ الشرعية الجنائية، متكلا على تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها.،وعليه خصصنا هذا المبحث إلى،القوانين العامة الموضوعية المتعلقة بالجريمة الإلكترونية(أ)، قانون الإجراءات الجزائية (ب).

أ- القوانين العامة الموضوعية المتعلقة بالجريمة الإلكترونية:

قد أخص المشرع الجزائري تنظيم الجريمة الإلكترونية بقوانين عامة وأخرى خاصة، وعليه قسمنا المطلب الأول، الدستور(1)، القانون العقوبات(2)،قانون الإجراءات الجزائية(3)

1- الدستور الجزائري:

كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016[1] حماية الحقوق الأساسية و الحريات الفردية، و على أن

---

[1] القانون رقم 16-01 المذكور سابقا.

تضمن الدولة عدم إنتهاك حرمة الإنسان. و قد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات و الإجراءات الجنائية وقوانين خاصة أخرى و التي تحظر كل مساس بهذه الحقوق. ومن أهم المبادئ الدستورية العامة :

المادة 38 : الحرّيّات الأساسيّة وحقوق الإنسان والمواطن مضمونة.

المادة44 : حرّيّة الابتكار الفكريّ والفنّي والعلمي مضمونة للمواطن. حقوق المؤلّف يحميها القانون. لا يجوز حجز أيّ مطبوع أو تسجيل أو أيّة وسيلة أخرى من وسائل التّبليغ والإعلام إلاّ بمقتضى أمر قضائيّ.الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون. تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.

لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون، سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة". أن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائي.

2- قانون العقوبات:

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون بموجب القانون العقوبات رقم 04-15 المؤرخ – في 10 نوفمبر 2004 المتمم لأمر رقم- 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات " ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394المادة مكرر7.

وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون- رقم 06-23 المؤرخ في 20 ديسمبر 2006 حيث مس هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص، الواردة في هذا القسم من القانون 04-15 وربما يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث من الإجرام بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى وشيوع إرتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وإنتشار الأنترنت كوسيلة لنقل المعلومات.

3- **قانون الإجراءات الجزائية الجزائري.**

بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة. غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية[1].

كما نص على التفتيش في المادة 45 الفقرة 7من نفس القانون[2] المعدلة حيث أعتبر إن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث

---

[1] أنظر:المادة 37 من قانون الإجراءات الجزائية المعدل والمتمم بأمر رقم 15-02 مؤرخ فى 23 يوليو سنة 2015،يعدل ويتمم الأمر رقم 66-155 المؤرخ فى 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية،الجريدة الرسمية عدد 40.

[2] أنظر:المادة 45 من قانون الإجراءات الجزائية المعدل والمتمم بقانون رقم 06-22 في 20 84 ص 6.

الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطته المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 44 من فانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الالكترونية. ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6[1] وكذا على "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5/ 10[2]. كما أن قانون الإجراءات الجزائية نص على ألا يجوز ضبطها إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة. غير أنه طبقا لقانون الإجراءات المعدل و المتمم في الفصل الرابع تحت عنوان "في إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور". نصت المادة (65 مكرر5/3)على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن بالإعتراض و وضع ترتيبات تقنية دون موافقة المعنيين من أجل إلتقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة[3]. أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية[1].

---

[1] أنظر:المادة 51 من قانون الإجراءات الجزائية المعدل والمتمم بقانون رقـــــم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد 84، ص 7.

[2] أنظر: تمم الباب الثانى من الكتاب الأول بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 ص8،بفصل رابع

[3] انظر: القانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل و يتمم الأمر رقم155-66 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966. و المتضمن قانون الإجراءات الجزائية الجزائري. المادة 65 مكرر 3/5 "إذا أقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخذرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أوالإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف و كذا جرائم

ونتيجة لما سبق وجب أن تلتزم الحكومة الجزائرية بوضع تشـــريعات واضـــحة لمواجهـــة الجريمـــة الالكترونية وسرعة تطورهـــا وتـــوفير خبـــرات فنيـــة عاليـــة قـــادرة علـــى التعامـــل والتطـــور التكنولـــوجي للجريمـــة، كـــذلك تبني قـــوانين منظمـــة لتـــداول المعلومات عبر شـــبكة الانترنـــت بمـــا لا يخـــل وحريـــة تـــداولها وإدراج تعريفـــات محددة للجرائم الالكترونية في قانون الإجراءات الجزائية وقانون العقوبات.

التحقيق الرقمي.

إن مفهوم "تقنية التحقيق الرقمي" يعطي ديناميكية حديثة للتحقيقات القضائية. إلا أن الواقع أقل كثيرا من المأمول. في حين أن الجدل كان محتدما لسنوات عديدة على الاشكاليات الجديدة التي يثيرها العالم الرقمي، فإن حالة القانون الإيجابي في تناقض صارخ مع هذه الحركية. وعلى الرغم من بعض محاولات التأقلم من خلال إرادة تشريعية للتكيف مع هذا الفضاء الجديد المتمثل في الإنترنت، فإن التحقيق الجزائي متردد، في حين أن الشبكات الإجرامية فهمت مدى الفضاء المتاح لها[2].

الفساد، يجوز لوكيل الجمهورية المختص بأن يأذن بما يأتي: – وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص فى أماكن خاصة أو عمومية...".

[1] الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائرى، د. فضيلة عاقلي، أ/محاضرة "أ" جامعة باتنة–1– الجزائر. كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، ص 115.

[2] Olivier Violeau, Les techniques d'investigations numériques: entre insécurité juridique et limites pratiques, AJ Pénal, 2017, p.324.

هدفنا هنا ليس تقديم شامل لتقنيات التحقيق الرقمي. بل على النقيض من ذلك: بل بالأحرى يتعلق الأمر بعرض الاشكالات التي تواجه الممارسين اليوم. وعادة ما تستخدم تقنيات التحقيق الرقمي كوسيلة لجمع أدلة أو قرائن المشاركة في ارتكاب جريمة، أو لتحديد مكان المشتبه فيه الذي يكون في حالة فرار. وهي الآن ضرورية لإجراء التحقيقات بشكل سليم، وذلك إما لكون الفضاءات الرقمية تكون محلا للجريمة (المواد الإباحية الماسة بالأطفال أو الاتجار بالأسلحة أو المخدرات، إلخ)، أو لأنها تستخدم كوسيلة للاتصال لايصال تعليمات في إطار ارتكاب هذه الجرائم.

مما سبق يتضح لنا أن الدليل الرقمي ينفرد بخصائص ومميزات تميزه عن سائر الأدلة المادية والعلمية والفنية، فلا شك بأن الدليل الرقمي كلما أحيط بمجموعة من الشروط والضمانات ووسائل التوثيق التي تكفل سلامة المعلومات والبيانات والدلائل المقرؤة والمحللة الكترونيا المنقولة والمثبتة عبر الوسائل والأجهزة الالكترونية وسلامة ودقة صحة نسبتها إلى صاحبها، فلا شك أنها تتمتع بالأصالة والاستقلالية عن الأنواع الأخرى وبالتالي يشير ذلك إلى عدة عوامل ومشاكل قانونية حول مدى شمولية مثل هذه الأدلة الرقمية بالقوانين والأنظمة والتشريعات الصادرة بشأن الأدلة المادية الأخرى، فطالما أننا اعترفنا بأنها تعتبر شكلا جديدا ومتفردا من أشكال الأدلة فهذا بلا شك يتبعه اعتراف بأهمية حاجتها لاجراءات ومواصفات تنظيمية تتناسب مع طبيعة خصائصها وأهميتها.

ويقصد بالحجية هي وصف ثابت بحكم الشرع يلحق مضمون الحكم القضائي أو الأمر القضائي فيه ويكون غير قابل للمناقشة فيه مرة أخرى.

ومعنى الحجية عند الفقهاء هي حجية الشيء المحكوم فيه أو عدم نقضه، معناها عند الفقهاء هو أن القاضي إذا عرضت منازعة أمامه في موضوع ما وتنازع الخصوم فيه وفحص القاضي أدلة كل خصم ومستنداته ووزنها ثم قال

كلمته الفاصلة في موضوع هذه الدعوى فلا يجوز لأي من الخصوم أن يعيدوا عرض النزاع مرة ثانية لمناقشة ما سبق أن فصل فيه[1].

ويمنع القاضي الذي أصدر الحكم أن يعدل عنه طالما استوفى الحكم شروطه ومتطلباته الشرعية لأن هذا الحكم هو رمز الصواب والصحة وهو عنوان الحقيقة، وما قيل عن حجية الحكم القضائي يقال كذلك عن حجية الدليل الرقمي.

أولا: الوصول إلى الدليل الرقمي.

1. استغلال معدات الحاسوب: إن استغلال معدات الحاسوب من بين الأدوات الأولى المتاحة للقضاة والمحققين، سواء أكانت حواسيب أو وسائط تخزين، وهو أمر ضروري لإظهار الحقيقة. سواء كانت بطلب من قاضي التحقيق أو النيابة، فإن الخبرة في مجال الاعلام الآلي تكون معيبة بشكل كبير: فالطرف الذي يستغل الوسيط الرقمي ليس هو الذي يجري التحقيق. ونظرا لكمية المعلومات التي يتم اكتشافها (عدة تيرابايت)، يكون من الضروري معرفة البيانات التي من المرجح أن تشكل دليلا على ارتكاب جريمة. يكون ذلك واضحا أحيانا، لا سيما عندما يتعلق الأمر باستغلال الأطفال في المواد الإباحية أو الاتجار بالأسلحة. لكن يكون الأمر أكثر صعوبة في سياق مراسلات عبر البريد الألكتروني يتم التطرق فيها بصورة عرضية إلى الدافع وراء ارتكاب جريمة.

على أية حال فإن هذه الخبرة على أجهزة الكمبيوتر سرعان ما تثبت محدوديتها، في زمن الحوسبة السحابية والتخزين عن بعد للبيانات. في الواقع، فإن الخبرة الكلاسيكية حسب جاءت به أحكام قانون الاجراءات الجزائية، تهدف إلى استغلال البيانات الموجودة فعليا في الأجهزة وليست المخزنة في خوادم

---

[1] الحمادي حسن، عقود و خدمات المعلومات، دراسة في القانون المصري والفرنسي، دار الثقافة للنشر و التوزيع، عمان، الأردن، الطبعة الأولى، 2003، ص 71.

أخرى. ولذلك فإن الوصول إلى هذه البيانات يدخل في إطار قانوني آخر لا يسهل اجراءات التحقيق.

2. الطابع غير المادي لوسائط تخزين المعلومات:

إذا انتقلنا بـــ " إدمون لوكارد[1] " إلى عالمنا المعاصر، يمكنه أن يفهم أن المشتبه فيه قد تم التعرف عليه من خلال خلية واحدة فقط خلّفها وراءه. لكن أن نشرح لرائد من رواد الشرطة العلمية أن آثار الجريمة أصبحت اليوم غير ملموسة سيكون تحديا[2].

إن المادة 5 من القانون رقم 09/ 04 هي التي توفر الإطار القانوني الأنسب لاستغلال هذه البيانات، حيث قررت على أنه يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى: منظومة معلوماتية أو جزء منها وكذلك المعطيات المعلوماتية المخزنة فيها ومنظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة– أ– من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

---

[1] إدمون لوكارد (Edmond Locard) أستاذ الطب الشرعي وهو من أسّس أول مخبر للشرطة العلمية في العالم في مدينة ليون الفرنسية في سنة 1910.

[2] Cédric Michalski, La recherche et la saisie des preuves électroniques, Gazette du Palais - 11/02/2014 - n° 042.

وإذا تبين مسبقا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

لقد جانب المشرع الجزائري الصواب عندما اقتبس هذه المادة في مجملها عن المشرع الفرنسي، حيث يقصد هذا الأخير بـــ "الاتفاقيات الدولية ذات الصلة": اتفاقية بودابست لمكافحة الجرائم المعلوماتية الموقعة في 23 نوفمبر 2001 تحت رعاية مجلس أوروبا، التي لم تصادق عليها الجزائر، مما يجعل هذا الاقتباس بدون موضوع.

ثانيا: الفعّالية المحدودة لتقنيات التحقيق الرقمي.

ويتعلق الأمر تحديدا باعتراض المراسلات الذي لا يمكن أن يتحقق لأسباب غامضة ذات طابع تقني أساسا، عندما تتم هذه المراسلات عبر تطبيقات المراسلة المشهورة حاليا. في عالم متصل بشكل مفرط، حيث يمكن أن ترسل رسالة مكتوبة عبر متعامل الهاتف، ولكن أيضا عبر واتساب، فايبر وغيرها من التطبيقات التي تقع خوادمها بشكل رئيسي في الولايات المتحدة الأمريكية، حيث تلجأ مصالح الأمن أولا إلى طلب "تجميد البيانات" من السلطات الأمريكية، ثم بناء على طلب المساعدة القضائية الدولية، تلتمس منها تسليم هذه البيانات، ولا تتلقى الرد إلا بعد عدة أشهر، وحتى دون التطرق إلى اشكالية فك تشفير البيانات، فإن الصعوبة التي يواجهها حاليا القضاة والمحققون تتعلق أساسا بهذا القيد التقني.

تنشأ صعوبة عملية أخرى لاعتراض المراسلات وكذلك لاسترجاع البيانات المخزنة فيها دون علم صاحبها. حيث أن التحقق المزدوج من الهوية للوصول إلى هذه المراسلات ضروري. وإن الوصول إلى البيانات يتطلب وجود تعاون

مقدمي خدمات البريد الإلكتروني، وهو أمر غير وارد في الوقت الراهن: فالحماية من تدخل السلطة العامة في الحياة الخاصة أصبحت حجة تجارية لهذه الشركات – والتي تتملّك البيانات الشخصية لأغراض تجارية أساسا. فالعولمة تسمح لهم بصفة خاصة بالتوطن في الدول التي لا تسمح تشريعاتها بإجبارهم على المساهمة في التحقيق الجنائي.

ثالثا: شروط قبول الدليل الرقمي كدليل إثبات في الجريمة المعلوماتية.

إنّ توسّع نطاق الجريمة الالكترونية يتطلّب تجديد أساليب إدارة الأدلة الجنائية التي تحتل مكانا استراتيجيا خاصا في المحاكمة نظرا لتعلقها بقناعة القاضي الشخصية. وقد أدى تطور التكنولوجيات الرقمية إلى تغيير أساليب التحقيق بحيث أصبحت الإجراءات الجزائية والتحقيقات متعلقة الآن باستغلال البيانات المستخرجة من جميع الوسائط الرقمية[1].

إن الأدلة المتحصلة عن الآلة تثير إشكالية عدم قبولها لدى القضاء نييجة عدم تعبيرها عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزييف والتحريف والأخطاء المتعددة وسرعة إتلافها أو تغييرها ولم يقيدها المشرع الجزائري بشروط خاصة بل تركها للقاضي.

لذلك يتعين على القاضي لقبول هذه الأدلة كأساس تستند إليه الحقيقة في الدعوى العمومية سواء أكان الحكم فيها بالإدانة أو بالبراءة توافر بعض الشروط أهمها:

1. أن تكون هذه الأدلة يقينية: وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات.

---

[1] Myriam Quéméner, Les spécificités juridiques de la preuve numérique, AJ Pénal 2014, p.63.

2. يتعين مناقشة الدليل الرقمي تطبيقا لمبدأ شفوية المرافعة: فإذا كانت مخرجات الوسائل الالكتررونية تعد أدلة إثبات قائمة في أوراق الدعوى في الجريمة المعلوماتية، فانه يجب مناقشتها أمام الخصوم إذ تنص المادة 212 من قانون الإجراءات الجزائية الجزائري في فقرتها الثانية على أنه:

" لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه ".

وهذا يعني أنه للقاضي الاجتهاد في الحكم في اجرائم المعلوماتية وعدم الاعتماد على رأي الغير، إلا إذا كان هذا الغير من الخبراء، وقد ارتاح ضميره إلى التقرير المحرر من طرفه

وقرر الاستناد إليه ضمن حكمه وبناء عليه يكون متولدا من عقيدته وليس من تقرير الخبير.

3. يجب أن يكون الدليل الرقمي مشروعا: ويقصد بذلك أن إجراءات جمع الأدلة الرقمية المتحصلة من الحاسب الألي إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجزائية.

ثانيا: سلطة القاضي في قبول الدليل الرقمي.

تتنوع نظم الأدلة الجزائية في الإثبات بين التي تأخذ بنظام الأدلة القانونية في الإثبات، وأخرى تعتنق نظام الإثبات الحر والقائم على حرية القاضي الجزائي في تكوين اقتناعه وتلك التي تجمع بين النظامين بما يسمى النظام المختلط.

ففي نظام الأدلة القانونية يتقيد القاضي في الإثبات بأدلة يحددها له المشرع مقدما ويقدر له قيمتها في الإثبات، فيتقيد القاضي بأن يستمد اقتناعه من هذه الأدلة دون غيرها[1].

---

[1] سعيد عبد اللطيف، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، مصر، 1999، ص149.

أما في نظام الأدلة الاقتناعية فان القاضي لا يقيده المشرع بأدلة إثبات معينة، وإنما يترك له حرية الإثبات وفقا للسلطة التقديرية في تقدير الدليل ويترتب عن ذلك أن للقاضي اجزائي قبول أي دليل يمكن أن يتولد منه اقتناعه[1].

وعلى الرغم من سيادة هذا النظام الأخير للإثبات الجزائي في جل التشريعات، منها الجزائر إلا أن المشرع قد طبق في إثبات بعض الجرائم نظام الأدلة القانونية عندما نص على تقييد سلطة القاضي في الإثبات بأدلة معينة ومثال ذلك إعطاء حجية كاملة لبعض المحاضر كمحاضر الحجز والمعاينة اجمركية التي تكون صحيحة إلى أن يثبت العكس، وهنا ينتقل عبء الإثبات من النيابة إلى المتهم ومثال ذلك الاعترافات والتصريحات في المحاضر الجمركية[2].

وإذا كان التطور العلمي قد أفرز ثورة الاتصالات عن بعد وجاءت للبشرية بتكنولوجيا جديدة نراها في مختلف مناحي الحياة، فالدليل مهما تقدمت طرقه وعلت قيمته العلمية أو الفنية في الإثبات، فانه يحتاج إلى قاض يتمتع بسلطة تقديرية، لأن هذه السلطة التقديرية تكون لازمة لتنقية الدليل من الخطأ أو الغلط أو الغش، وهي تكون ضرورية أيضا لكي تجعل الحقيقة العلمية حقيقة قضائية.

كما يسيطر على الإثبات الجنائي في قانون الإجراءات الجزائية مبدأ حرية القاضي في الاقتناع ذلك أن نص المادة 212 من قانون الإجراءات الجزائية تنص على جواز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ولا يوجد نص خاص في القانون يقيد مبدأ الإثبات الجنائي في مواد الجريمة المعلوماتية فتخضع بذلك للقواعد العامة في الإثبات.

---

[1] عبد الرؤوف مهدي، حدود حرية القاضي في تكوين عقيدته، مؤسسة العين للطباعة، دون دار للنشر، دون سنة الطبع، ص12.

[2] د. أحسن بوسقيعة، المنازعات الجمركية، دار هومة، الطبعة الثانية، 2005، ص191.

وللقاضي وعلى الرغم من أنه يتمتع بالحرية في تكوين عقيدته إلا أنه ملزم بتسبيب حكمه وبيان الأدلة التي استمد منها اقتناعه، فليست الحرية أن نطلق العنان لكي يقتنع بما يحلو له، وإنما هو حر فقط في استخلاص الحقيقة من مصدر مشروع.

وبالنظر إلى الطبيعة الخاصة التي تتميز بها الأدلة المتحصلة من الوسائل الالكتررونية وما قد يصاحب الحصول عليها من خطوات معقدة، فان قبولها في الإثبات قد يثير العديد من المشكلات، ذلك أنه يمكن التلاعب فيها وتتغير الحقيقة التي بجب أن تعبر عنها.

ولذلك فان المشكلات التي تثيرها هذه الأدلة ليس بسبب أنها قد تصلح لتكون طرق إثبات أم لا، وإنما المشكلة التي تتعلق بها تتحدد في كيفية ضمان مصداقية هذه الأدلة ومدى تعبيرها بالفعل عن الحقيقة التي تهدف إليها الدعوى العمومية في هذا النوع من الجرائم.

وهذه الأدلة المتحصلة من الوسائل الالكترونية تخضع للسلطة التقديرية للقاضي الجزائي، فان استراح إليها ضميره ووجدها كافية ومنطقية فيمكنه أن يستمد اقتناعه ويسبب حكمه بالاعتماد عليها.

وفي الجزائر فإن الأدلة المتحصلة من الوسائل الالكترونية كأدلة إثبات يسودها مبدأ حرية القاضي في تكوين اقتناعه، فهو يتناول حجية الأدلة الرقمية ضمن مسألة قبول الأدلة المتحصلة من الآلة أو ما يسمى بالأدلة العلمية والتي تقبل كطرق إثبات حسب نص المادة 212 من قانون الإجراءات الجزائية.

فالمشرع الجزائري لم يضع أي نصوص قانونية صريحة بهذا الخصوص حيث تم الاستناد في هذا الموضوع للمادة 212 من قانون الإجراءات الجزائية الجزائري السابق الإشارة إليها، والتي طبق من خلالها مبدأ حرية الإثبات، لكن

المشرع أدرك أن هذا لا يكفي لوحده، وليواكب التطور الحاصل فيما بعد وضع القانون رقم 15/04 المؤرخ في 10 نوفمبر سنة 2004 المتمم والمعدل للأمر 66/156 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات "، ولقد جاء في عرض أسباب هذا التعديل مواكبة التطور التكنولوجي والمعلوماتي وانتشار وسائل الاتصال الحديثة التي أدت بدورها إلى ظهور أشكال جديدة للإجرام، وكان يهدف هذا القانون إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وكان هذا القانون كنتيجة حتمية لما أفرزته ثورة تقنية المعلومات التي مست مصالح جديدة غير تلك التي يحميها قانون العقوبات، فقد تطرق المشرع الجزائري إلى تجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات من خلال تعديل قانون العقوبات بموجب القانون 15/04 والذي تضمن ثمانية مواد تطرق المشرع من خلالها إلى حماية سرية وسلامة المعلومات ونظم معالجتها وذلك من المواد 394 مكرر إلى 394 مكرر 7، أين جرم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه[1].

بعدها تدخل المشرع الجزائري لحماية الاتصالات الرقمية حين وضع القانون رقم 09/04 المؤرخ في 5 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومن خلال هذا القانون أدرج المشرع طريقة ضبط الأدلة الرقمية والتي تتخذ صورتين: الصورة الأولى تكمن في نسخ المعطيات محل البحث عن تخزين المعلومات الرقمية على أن تكون هذه المعطيات مهيأة بشكل يجعلها قابلة لحجزها ووضعها في أحراز

---

[1] القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات اجزائية، والصورة الثانية تتمثل في الاستعانة بالتقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي تحويها هذه المنظومة أو القيام بنسخها، ويكون ذلك في حالة صعوبة الحصول على هذه الأدلة وفقا للصورة الأولى.

وهذا يعني أن الدليل الرقمي يخضع في ضبطه وتحريزه إلى قواعد تحريز الأدلة الجنائية عموما، إلا أنه ونظرا إلى الطبيعة الخاصة له فان عملية الحصول عليه تحتاج لبعض الإجراءات الخاصة التي تحافظ عليه وتحميه من العبث به وتغييره، وهذا ما أشارت إليه المادة السادسة (6) في فقرتها الثالثة (ج) من القانون رقم 09/04 والتي تلزم السلطات المعنية بعملية ضبط الدليل الرقمي أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، وأن لا يؤدي استعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات[1].

ونظرا لأهمية وسائل التحقيق والتحديات المرتبطة بالعالم الرقمي، فمن المؤكد أن الوضع سيتطور بشكل كبير في السنوات القادمة. وقد بعثت أعمال القرصنة والمخاطر المالية الأخيرة على نطاق واسع الأمل في أوساط ممارسي التحقيق الجزائي في إمكانية توفير الموارد التقنية والبشرية الطموحة، حتى يتسنى لقضاء الغد أن يواجه تحديات المجتمع، والتي نجد الكثير منها في العالم الرقمي.

---

[1] محمودي نور الهدى، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد 11، جوان 2017، ص 908-926.

الممارسة القضائية الدولية في مواجهة المراقبة الرقمية.

بعد أن قرّر الرئيس الأمريكي متبوعا بالكنغرس، الحد من صلاحيات وكالة الأمن القومي NSA بشكل واضح. حيث أصبح جمع البيانات من اختصاص متعاملي الاتصالات الذين يتحصلون عليها مباشرة من زبائنهم. وبالتالي فإن قانون الحريّات Freedom Act لا يفسر نهاية جمع البيانات التي يمكن بعد ذلك تسليمها لمكتب التحقيقات الفدرالي FBI أو وكالة الأمن القومي، بعد الحصول على إذن مسبق من محكمة مراقبة الاستخبارات الخارجية FISA Court و بعد تحديد هدف معين. إذن هي نهاية الجمع الشامل للبيانات، بما في ذلك بيانات الاتصال بالإنترنت، ولكن يتعلق الأمر بالأميركيين فقط (فرع أول).

وفي سياق التطورات المتسارعة، أصبح موضوع "الرقمنة" وما يسمى " التقنيات الجديدة للمعلومات " (NTI) يشكل أهمية كبيرة ويطرح أسئلة أساسية على المجتمع. وبما أنه من الصعب مطابقة القواعد القانونية أو حتى جعلها ببساطة متوافقة من بلد إلى آخر، فإن القضاة مدعوون لاصدار قرارات تكون عواقبها عالمية. وهو حال أكبر الهيئات القضائية الأوروبية كمحكمة العدل الأوروبية CJCE أو المحكمة الأوروبية لحقوق الإنسان CEDH (فرع ثاني).

الخيار الأمريكي في هيئة قضائية مختصة.

عندما تم التصويت على قانون باتريوت آكت Patriot Act أو قانون مكافحة الإرهاب، أو قانون الوطنية، والذي تم إقراره في أعقاب اعتداءات 11 سبتمبر 2001، وهو خاص بتسهيل إجراءات التحقيقات و الوسائل اللازمة لمكافحة الإرهاب، والذي لقي استياء المراقبين الأجانب نظرا لطابعه المقيّد للحرّيات العامة. إن حجم هذا الحدث غير المسبوق سوف يبرر الحرب التي يعتزم جورج

بوش شنها ضد "محور الشر" (خطاب حالة الاتحاد في 29 ديسمبر 2002): في 14 سبتمبر يعلن حالة الطوارئ الوطنية ويوقع مرسوما يضع القوات المسلحة الاحتياطية تحت نظام نشاط معين. وفي الأيام التالية تم اعتماد قانون يضم أكثر من 300 صفحة بأغلبية ساحقة، يعدل على وجه الخصوص قانون مراقبة الاستخبارات الأجنبية الصادر عام 1978.

يتعارض محتوى قانون مكافحة الإرهاب الأمريكي مع الحقوق الموضوعية والإجرائية. وبوجه عام تم إنشاء أنظمة مراقبة جديدة ؛ من خلال تعميم تدابير اعتراض الاتصالات التي كانت تقتصر في السابق على حالات الاستثنائية. وإجمالا تمس آلية مكافحة الإرهاب على الأقل بستة بنود دستورية. وعلينا أن نعزل من أجل دراستنا القسم القديم رقم 802 الذي أعطى تعريفا واسعا بوجه خاص لنطاق القانون المطبق على النشاط الإرهابي. ويرتبط مفهوم "الإرهاب المحلي" بأي نشاط يهدد حياة الأفراد على الأراضي الوطنية و "يهدف إلى تخويف المدنيين أو التأثير على سياسة الحكومة من خلال الدمار الشامل والاغتيال أو عمليات الاختطاف...". وإن غموض هذا التعريف ينطوي على مجموعة من المخاطر بحيث أن هذه الاجراءات قد تشمل أنشطة لا علاقة لها مع الإرهاب بالمعنى المعتاد. وغموض هذا التعريف – بلا شك عمدي – أدى حتما إلى وقوع تجاوزات في الواقع. وبسبب المصطلحات المستخدمة فإن هذا النظام الذي كان من المفترض أن يكون استثنائيا أصبح بالامكان توظيفه في سياق قضايا القانون العام. ومن خلال تفسير موسّع إذن يمكن بالتالي وصف أي احتجاج سياسي بأنه "إرهاب داخلي" بينما منع البند الدستوري الأول الكونغرس من إصدار قوانين تقيد حرية التعبير. وحسب جمعيات الدفاع عن الحريّات، خاصة الاتحاد الأمريكي للحريات المدنية ACLU (American civil liberties union)، فإن مكتب

التحقيقات الفيدرالي FBI قد أفرط في توظيف هذه الإمكانية التي يتيحها القسم 802، ولم يكتفي باستعمالها في حالة العمل الإرهابي فقط.

ولذلك فإن المخاوف بخصوص تحديد نطاق واسع لمجال تطبيق القانون الجزائري، تستند إلى دروس مستخلصة من القانون المقارن. وسيكون من السذاجة الإجابة على أن أجهزة المراقبة لدينا ليست مكتب التحقيقات الفيدرالي FBI: حتى في الجزائر يمكن يوما ما للقواعد الاستثنائية أن تحيد عن النوايا الحسنة لمؤسسيها والتي نص عليها القانون رقم04 09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[1]ا.

وقد سبق خيار المحكمة الخاصة اعتماد قانون الحرّيات Freedom Act الذي حاول اضفاء الشفافية على الاجراءات القضائية، حيث تم إنشاء محكمة مراقبة الاستخبارات الخارجية بموجب قانون مراقبة الاستخبارات الأجنبية الصادر فى 1978. حقيقة أننا من الناحية المطلقة نؤيد التدخل القضائي قبل أي إجراء من إجراءات المراقبة. نعتقد أن إنشاء قاضي خاص ضروري لتفادي وقائع هي الأخرى خاصة، في عالم أصبح مختلفا. وهذا لا يعني بطبيعة الحال تصورا جديدا يتسم بتقييد الحرّيات، ولكن وسيلة محددة لمكافحة الإرهاب بجميع أشكاله، من خلال الجمع بينها وبين تعزيز وجود ضمانات لحماية الحريات. ومن جميع الضمانات تبقى الحماية القضائية هي الأقوى. إن الحدود بين المنع والقمع غامضة في هذا المجال بحيث يبدو التمييز بين الشرطة الإدارية والقضائية مصطنعا. وتعتبر أعمال الإرهاب جرائم مستقلة يعاقب عليها بالعقوبات المشددة (القسم الرابع مكرر تحت عنوان الجرائم الموصوفة بأفعال إرهابية أو تخريبية)

---

[1] القانون رقم 09-04 المذكور سابقا.

التي تخضع لنظام إجرائي خاص (محكمة جنايات مكونة حصريا من قضاة محترفين).

ولهذا السبب فإن إصدار التراخيص من أجل استخدام تقنيات المراقبة المتطورة والتطفلية لا ينبغي أن يكون من اختصاص السلطة التنفيذية بل من اختصاص القاضي وحده. أو على أقل تقدير من اختصاص السلطة التنفيذية ولكن بعد الحصول على إذن القاضي المختص و هذا ما نصت عليه المادة 4 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

هذا النظام بطبيعة الحال يمكن مقارنته بالاذن الذي تمنحه محكمة مراقبة الاستخبارات الخارجية FISA Court في الولايات المتحدة الأمريكية.

وهكذا يسعى قانون الحرّيات Freedom Act إلى زيادة تدابير الشفافية في الإجراءات أمام محكمة مراقبة الإستخبارات الأجنبية FISA Court (على وجه الخصوص، الباب الرابع من القانون، "إصلاحات محكمة مراقبة الاستخبارات الأجنبية"). وكذلك فإن القانون ينشئ فريقا جديدا من الخبراء الذين يمكن أن تستعين به المحكمة في ميدان الحقوق والحريات وتكنولوجيات الاتصال الجديدة. وعلاوة على ذلك، فإن القرارات الرئيسية للمحكمة أصبحت علنية، في حين أن الإجراءات أمامها كانت سرّية منذ إنشائها في عام 1978 بعد قضية واترغيت Watergate. ولكن إذا كان مبدأ مثل هذه المحكمة الخاصة يبدو مثيرا للاهتمام بهدف مقارنة محتملة أو حتى اقتباس، فإن حال الممارسة غير ذلك. ولا شك أن أحكام قانون الحرّيات الجديد المتعلقة بمحكمة مراقبة الإستخبارات الأجنبية FISA Court تستغرق وقتا لتخليصها من العبء الثقيل المتعلق بالماضي

الغامض، بعد قيام وكالة الأمن القومي NSA بأعمال مراقبة شاملة دون الحصول على الاذن القضائي اللازم مبدئيا[1].

المحكمة الأوروبية لحقوق الانسان جهة قضائية بملامح رقمية.

سنركز على عنصرين: حماية الحريات العامة ضد السلطات العامة ؛ وحماية البيانات الشخصية في مواجهة متعاملي القطاع الخاص.

أولا: حماية الحريات العامة في مواجهة السلطات العمومية.

سنأخذ مثالين لافتين للنظر على وجه الخصوص: قرار Digital Rights في قضية الاحتفاظ بالبيانات الذي يمكن إدراجه من ضمن القرارات الكبرى للمحكمة الأوروبية لحقوق الانسان ؛ وقرار Volker و Markus Schecke في قضية نشر البيانات.

فمن خلال قرار Digital Right و K�rntner Landesregierungs[2] وسّعت المحكمة الأوروبية من رقابتها على هامش التقدير الممنوح للسلطة التشريعية في مجال الحقوق الأساسية وحققت "سبقا قضائيا عالميا" في مجال الاحتفاظ بالبيانات وفي مجال الحرّيات العامة.

وفي أعقاب الهجمات الإرهابية في مدريد ولندن في عامي 2004 و 2005، أنشأ الاتحاد الأوروبي نظاما للاحتفاظ بحركة مرور البيانات بناءا على

---

[1] Wanda Mastor, La loi sur le renseignement du 24 juillet 2015 « La France, Etat de surveillance » ? AJDA 2015 p.2018

[2] CJUE, 8 avr. 2014, nos C-293/12 et 594/12: AJDA 2014-1147, chron. M. Aubert, E. Broussy et H.

التوجيه رقم CE/24/2006 الذي تم تبنيه على أساس المادة 95 CE في اطار تقريب التشريعات. وقد سبق أن أصدرت بعض الدول الأعضاء تشريعات بشأن هذا الموضوع بصفة مشتتة، وجرت مناقشة جدوى هذه التقنية في مكافحة الجرائم والتحقيق فيها وقمعها، ولا سيما فيما يتعلق بالجريمة المنظمة، وذلك منذ سنة 2002 من طرف مجلس العدل والشؤون الداخلية في الاتحاد الأوروبي. وكان الهدف هو إلزام مقدمي خدمات الإنترنت أو متعاملي الهاتف النقال بالاحتفاظ ببعض البيانات لفترة معينة من الوقت حتى يتسنى لمصالح الأمن الوصول إليها حسب الضرورة. وقد أخطرت المحكمة الأوروبية من طرف المحكمة العليا الايرلندية و المحكمة الدستورية النمساوية[1] بمسائل فرعية بشأن صحة النظام نفسه في أعقاب الاحتجاج على التشريعات الوطنية التي طبّقت التوجيه في أيرلندا والنمسا. وفي هذا البلد الأخير انضم أكثر من 11 000 مواطن إلى اقليم Carinthie من أجل تسجيل طعن أمام المحكمة الدستورية. تم قبول الطعن على مستوى محكمة العدل الأوروبية CJCE التي أقرّت بعدم قانونية النظام. ويبدو أن محكمة العدل الأوروبية كانت أول هيئة قضائية في العالم اتخذت موقفا بشأن المسألة.

لقد عاينت محكمة العدل الأوروبية مدى خطورة المساس بالحق في حرمة الحياة الخاصة والحق في حماية البيانات الشخصية، باتباع منهجية قريبة لتلك التي تتبعها المحكمة الأوروبية لحقوق الإنسان CEDH ، حيث مارست رقابتها على مدى توفر شرطي الضرورة والتناسب على أساس المادة 52 ف1[2] من

---

[1] Verfassungsgerichtshof .

[2] "يجب أن ينص القانون على أي تقييد بشأن ممارسة الحقوق والحريات التي يقرها هذا الميثاق، ويجب احترام جوهر تلك الحقوق والحريات، وفقاً لمبدأ التناسب – يجوز وضع القيود

ميثاق الحقوق الأساسية للاتحاد الأوروبي[1] المبدأ القائل بأن الرقابة القضائية يجب أن تكون "صارمة" في مسألة الحقوق الأساسية لأن هامش المناورة لدى السلطة التشريعية مقيّد أصلا[2]. ويتعين مقارنة هذا الحل مع قرار مجلس الدولة في قضية Benjamin الشهيرة [3] التي اعتبر فيها أن الأعمال التي تمس بالحريات العامة تخضع لرقابة قضائية شاملة والتي تسمى أيضا برقابة الملائمة[4].

فقط إذا كانت لازمة وتفي بشكل حقيقي بأهداف المصلحة العامة التي يقرها الاتحاد، أو الحاجة لحماية حقوق وحريات الآخرين".

[1] CEDH, gde ch., 4 déc. 2008, no 30562/04, S. et Marper c/ Royaume-Uni, § 102.

[2] La jurisprudence selon laquelle la Cour n'exerce qu'un contrôle restreint, de l'erreur manifeste d'appréciation, sur les choix normatifs du législateur de l'Union lorsqu'il intervient dans un domaine impliquant de sa part des choix de nature politique, économique et sociale, dans lesquels il est appelé à effectuer des appréciations complexes ne joue donc pas. Jean-Claude BONICHOT, La cour de justice de l'Union européene et les nouvelles
technologies de l'information: vers une cour 2.0 ? Petites affiches - 15/03/2016 - n° 53 - page 8.

[3] Commentaire de l'arrêt Benjamin, 19 mai 1933, Les grands arrêts de la jurisprudence administrative, 2015, 20e éd., p. 266).

[4] أتجه مجلس الدولة الفرنسي في هذه القضية الى الاستقرارعلى حقه في بحث وتقدير مدى خطورة الافعال او الوقائع التي تهدد النظام العام ومدى تناسبها مع إجراءات الضبط الاداري المتخذة بناء على هذا التهديد والتي تقيد بها سلطات الضبط الحريات العامة المكفولة بنصوص دستورية او قانونية، حيث اخضع إجراءات الضبط الاداري المقيدة لتلك الحريات لرقابة الملاءمة من حيث تناسب الأجراء مع السبب الذي يسمح لهيئات الضبط التدخل لحماية النظام العام او صيانته عند تعرضه للخطر، وهكذا استقر مجلس الدولة الفرنسي في مجال حرية الاجتماعات العامة بعدم الاكتفاء بالرقابة على الوجود المادي للوقائع او حتى تكييفها القانوني بل توسع بهذه الرقابة ليصل الى بحث عنصر الملاءمة في القرار الضابط، لينتهي في الغالب الى عدم اقرار سلطة الضبط في إصدارها لقرارات منع الاجتماعات العامة رغم توقع حدوث

وفيما يتعلق بمدى المساس بحرمة الحياة الخاصة والبيانات الشخصية، عاينت المحكمة أن النظام المستخدم يسمح بمعرفة مع من وكيف تم الاتصال ومدته ومكانه وكذلك تواتر الاتصالات مع مراسل معين في فترة محددة. جميع هذه العناصر تعطي مؤشرات دقيقة على الحياة الخاصة للأفراد. واعتبرت المحكمة أن ذلك قد يخلق " شعورا منتشرا بالمراقبة المستمرة".

ما هي تبعات قرار محكمة العدل الأوروبية؟ إذا كان قرار Digital Rights يعترف بالمصلحة العامة قد تبرر الاحتفاظ ببيانات الاتصال بشروط معينة، فإنه يمنع بوضوح "الاحتفاظ الشامل" بها، أو ما يسميه البعض بالاحتفاظ الأعمى. ولذلك يجب أن يكون الاحتفاظ بالبيانات مصحوبا بضمانات. وهذا يعني على الأقل توفر المتطلبات التالية: استهداف الحالات التي يمكن فيها فرض الاحتفاظ بالبيانات، على سبيل المثال للكشف عن جرائم محددة ومتابعة مرتكبيها ؛ والحد من عدد البيانات التي يتعين الاحتفاظ بها ؛ وتحديد مدة الحفظ ؛ أن ينظم في التوجيه نفسه على أن الوصول إلى البيانات لا يمكن أن يتم إلا بقرار سلطة إدارية مستقلة أو حتى قضائية ؛ النص على أن يتم الاحتفاظ بالبيانات على أراضي الاتحاد.

بعد أن تطرقنا إلى مسألة الاحتفاظ بالبيانات، نتطرق في مرحلة ثانية إلى مسألة نشرها.

يعتبر قرار Volker und Markus Schecke و Eifert[1] المثال الأول عن صعوبات التوفيق بين مبدأ الشفافية واحترام حرمة الحياة الخاصة. وكان

خلل او اضطراب بالنظام العام طالما كان عليها اتخاذ التدابير والاحتياطات اللازمة للحيلولة دون وقوع هذا الخلل او الاضطراب.

[1] Arrêt de la CJUE du 9 novembre 2010. Volker und Markus Schecke GbR (C-92/09) et Hartmut Eifert (C-93/09) contre Land Hessen.

السؤال المطروح في ما إذا كان بإمكان المشرع الأوروبي أن يسمح بنشر على موقع على شبكة الإنترنت أسماء المستفيدين من المساعدات الفلاحية وكذا مبالغ المساعدات التي يتلقونها. وقد اتخذت هذه المبادرة في أعقاب انتقاد للسياسة الفلاحية المشتركة (PAC). وكانت الفكرة هي أنه ستكون مقبولة على نحو أفضل من قبل المواطنين إذا وضعت جميع المبالغ المدفوعة على الطاولة، بهدف وضع حد للتجاوزات. وقد ترجمت إلى قوانين صادرة عن المجلس والمفوضية. وقد قام المكتب الفدرالي للزراعة والأغذية بتطبيق هذه السياسة: فقد تضمن موقعه على شبكة الإنترنت أسماء المستفيدين من المساعدات، والبلدية التي يقيمون فيها مع رمزها البريدي، ومبالغ المساعدات التي تلقوها، مع اضافة محرك بحث... اشتكى المعنيون من الإزعاج الذي سببه لهم هذا التشهير في الحياة اليومية: فضول زائد، تعليقات مهينة من البعض... هل انتهك هذا النظام الحق في حرمة الحياة الخاصة والحق في احترام حماية البيانات الشخصية؟

إن إجابة المحكمة جاءت متباينة. بالنسبة للأشخاص الاعتبارية فإنها لا تتمتع بالحماية المنصوص عليها في المواد 7 و 8 من الميثاق إلا إذا حدد الاسم القانوني للشخص الاعتباري شخصا طبيعيا واحدا أو أكثر. كما هو الحال بالنسبة لشركة Volker und Markus Schecke و Eifert[1]. أما بالنسبة للأشخاص الطبيعية فإن الحماية تكون كاملة. و لمحكمة العدل الأوروبية وجهة نظر صارمة والتي تتماشى مع اجتهاد المحكمة الأوروبية لحقوق الانسان. ومن ثم فإن حماية حرمة الحياة الخاصة تغطي حتى البيانات المتعلقة بالأنشطة المهنية وإشعار مسبق

[1] Arrêt de la CJUE du 9 novembre 2010. Volker und Markus Schecke GbR (C-92/09) et Hartmut Eifert (C-93/09) contre Land Hessen.

بسيط بأن البيانات من المرجح أن تنشر لا يمكن اعتباره بمثابة موافقة من طرف الأشخاص المعنية.

حقيقة أن المساس بهذه الحقوق يمكن تبريره بالهدف الذي يسعى إليه التنظيم المعني المتمثل في تطبيق مبدأ الشفافية وفي الرقابة العمومية على استعمال الأموال الأوروبية. غير أن المحكمة ترى أن هناك اختلال في التوازن بين المصالح العامة وحقوق الأشخاص الطبيعية المعنية لعدة أسباب. أولا بسبب الطريقة التي تم بها انشاء النظام: الوصول الشامل والسهل إلى البيانات عبر مواقع الانترنت للدول الأعضاء، دون تمييز بين حجم المبالغ أو فترات و عدد المساعدات ودون تفرقة بين مختلف أنواع المساعدات. وتشير المحكمة أيضا أنه كان ينبغي اغفال البيانات المتعلقة بالمبالغ الصغيرة. لكن هذه الاعتبارات لا تنطبق على الأشخاص الاعتبارية لأنها في كل الأحوال تخضع لالتزامات واسعة بنشر بيانات مختلفة تتعلق بها.

تعتبر حماية الحقوق والحريات من بديهيات قانون الدول الأعضاء في الاتحاد الأوروبي وكذلك هو الحال في قانون الاتحاد. ولكن تطور المجتمع يظهر بشكل كبير أنها مهددة بقدر أكبر من طرف الخواص، الشركات الكبرى على وجه الخصوص. واليوم بشكل واضح من طرف عمالقة شبكة الانترنت. و يقدم اجتهاد محكمة العدل الأوروبية بخصوص ذلك صورا نموذجية.

ثانيا: حماية البيانات الشخصية في مواجهة متعاملي القطاع الخاص.

لا يخفى على أحد أن الخواص بما في ذلك الشركات، مهددون بسبب سلوك متعاملي القطاع الخاص. ويرجع ذلك إلى سبب البسيط يتمثل في أن الإنترنت يكسر جميع الأطر القانونية وغيرها في الحياة الاجتماعية والاقتصادية. والواقع أنها تتيح التحرر من كل شيء وبصفة خاصة من احترام القاعدة القانونية.

يهدد عمالقة الانترنت الحياة الخاصة وفي مواجهة هذا التهديد جاءت اجابة القرار المشهور في السنوات الأخيرة: Google Spain. وهو يتعلق ما يسمى "الحق في النسيان". وقد صدر حكم Google Spain على أساس التوجيه رقم 46/95 المؤرخ 24 أكتوبر 1995 المتعلق بحماية البيانات الشخصية. وهذا يبين أن النظام العام لهذا التوجيه القديم[1] لا زال صالحا في مواجهة التحديات الناشئة عن ظهور عمالقة متعددي الجنسية والمعروفين على الإنترنت.

وكانت لهذه القضية نقطة بداية تمثلت في حالة المحامي Mario Costeja Gonz□lez. عند إدخال اسمه على محرك البحث غوغل، نجد مقالين نشرا في عام 1998 أعلنا عن بيع في المزاد العلني لمبنى ملك له كان موضوعا لرهن عقاري. وفي عام 2010 طلب المعني من السلطة الإسبانية لحماية البيانات حذف نتيجة هذا البحث. وطلب من جهة أن تقوم الصحيفة المعنية La Vanguardia، بحذف وقائع المنازعة، ومن جهة أخرى أن يجعل غوغل هذه النتائج غير مرتبطة بنتيجة البحث عن اسمه. لم تستجب السلطة الإسبانية لطلبه فيما يتعلق بالصحيفة الإلكترونية على أساس أنها لم تقم إلا باعادة نشر إعلان قانوني عن النسخة الورقية. لكنها استجابت لطلبه في مواجهة غوغل.

وفيما يتعلق بالتوازن الذي ينبغي تحقيقه بين حماية الحياة الخاصة والمصالح الاقتصادية لشركات الإنترنت وحق مستخدمي الإنترنت في الاعلام، أقرّت محكمة العدل الأوروبية بعنصرين هامين. أولا وبالنظر إلى اتساع وتنوع المعلومات التي يتيحها محرك البحث للجمهور، فإن المساس بحقوق الشخص المعني لا يمكن أن تبرّره المصلحة الاقتصادية للمتعامل. وثانيا تتفاوت التزامات المتعامل وفقا للشخص المعني، حيث يجب قياسها من حيث طبيعة المعلومات، وبالتالي حسب حساسيتها بالنسبة للحياة الخاصة للمعني ومن حيث مصلحة الجمهور في الاطلاع عليها. وبالتالي فإن الحياة الخاصة للرجل السياسي أو النجم

---

[1] رغم مرور 22 سنة على تبني هذا التوجيه الأوروبي، إلا أنه في المقابل لم يتم لحد كتابة هذه السطور في الجزائر تبني قانون لحماية البيانات الشخصية.

السينمائي تكون بالتأكيد أقل حماية من مستخدمي الإنترنت بالمقارنة مع حياة الفرد بشكل عام.

وكما تصورته المحكمة فإن "الحق في النسيان" عنصر من حق أعم في عدم الكشف عن الهوية. وهو لا يتعلق فقط بالمعلومات الكاذبة ولكن أيضا بالمعلومات الصحيحة التي نقلت في وقتها بصفة قانونية إلى معرفة الجمهور ولكن مصلحة الجمهور فيها ضعيفة بينما يكون الضرر الذي قد يلحق الشخص المعني كبيرا. ولذلك فإن قرار غوغل يحمي حرمة الحياة الخاصة بشكل كبير، لأنه يرجح الكفة لصالح الفرد، في مواجهة حق مستخدمي الإنترنت في الاعلام، وفي مواجهة حرية المتعامل في المبادرة الاقتصادية.

ما الذي ترتب عن هذا الحكم؟

تفاعل غوغل بسرعة مع قرار محكمة العدل الأوروبية حيث وضع تحت تصرف الجمهور استمارة إلكترونية لطلب إزالة نتائج البحث مباشرة عبر الإنترنت. طلبات الإزالة ومصيرها تكون موضوع الإحصائيات التي ينشرها غوغل في اطار تقريره "شفافية المعلومات"[1].

في 6 فبراير 2015 نشرت المجموعة الاستشارية التي أنشئها غوغل تقريرا يوصي بأن ينحصر حذف الروابط المثيرة للجدل في النسخ الأوروبية لمحرك

---

[1] وحسب ما جاء فى موقع "تورنت فريك"، فإن شركة غوغل استقبلت أكثر من 345 مليون طلب لإزالة روابط متعلقة بمواد مقرصنة من نتائج محركها للبحث خلال عام 2014، أى أنها كانت تقريبا تتعامل مع مليون طلب بشكل يومى. يشار إلى أن 2014 مثلت طفرة كبيرة فى عدد طلبات إزالة المحتوى التى تتلقاها غوغل سنويا بالمقارنة مع 62 طلبا فقط عام 2008.
ووفقا لتقرير الموقع فإن مواقع تبادل الملفات 4shared.com و Rapidgator.com
Uploaded.net كانت الأكثر استهدافا من قبل أصحاب ومالكي المواد الأصلية بإجمالي 5 ملايين طلب تقريبا لكل موقع. فيما كانت مجموعة BPI الموسيقية البريطانية الأكثر تقدما بطلبات الإزالة لحماية مواد خاصة بها عبر أكثر من 60 مليون طلبا للإزالة.

البحث. ومع ذلك فقد كانت مجموعة "المادة 29" قد أوصت السلطات الوطنية لحماية البيانات في نوفمبر 2014 بأن لا تقتصر إزالة الروابط على الإصدارات الوطنية لغوغل، بل تمتد أيضا إلى google.co

الخاتمة

يبدو أن الحريات العامة تعاني كثيرا من المقاربة الحالية التي تنتهجها الحكومات وتشريعات العالم والتي تتلخص في أن هدف الأمن العام يبرر القيود المفروضة على حقوق الأفراد. ومع ذلك فإن احترام حرية التعبير والإعلام يلعب دورا حاسما في الحفاظ على الديمقراطية والتنمية البشرية المستدامة وتعزيز السلم والأمن الدوليين. أدت الإجراءات الأمنية ولا سيما في مجالات الإرهاب والهجرة إلى تقويض الحقوق الفردية ونتج عنها قيود غير قانونية على الحق في حرية التعبير واستهداف جماعات عرقية ودينية معينة. لذا أصبح من الضروري اليوم استبعاد فكرة أن الأمن يتطلب اعادة النظر في حقوق الإنسان. على العكس من ذلك فاحترام الحقوق الأساسية ضروري لتحقيق الأمن الحقيقي.

للفهم الجيّد اللعلاقة بين الأمن والحريات العامة، من الضروري أولا تقبل حقيقة أن مفهوم الأمن العام، على النحو المنصوص عليه في التشريعات والممارسة الإدارية الحديثة، مفهوم خطير ويحمل عواقب حقيقية وخطيرة على ممارسة الحريات العامة – سواء من الناحية الدستورية والسياسية والقانونية والمؤسساتية أو الديمقراطية. ولذلك يمكن اعتبار وبشكل أساسي أن هذا المفهوم يتعارض مع آليات ديمقراطية ليبرالية، لا سيما وأنه يشكل غموضا منقطع النظير وتسمح مرونته باستخدامه تحت أشكال مختلفة تبعا للظروف.

يستخلص مما سبق أن العديد من التحديات تواجه المبادئ والمؤسسات والممارسات الاجتماعية، من اللحظة التي نريد فيها ومهما كان الثمن التوفيق بين الحرية والأمن وهذه التحديات لا تستثني الوسط الرقمي، لا بل يزيد هذا الأخير من درجة التوتر. على هذا النحو تتعرض حرية التعبير لانتهاكات من اللحظة

التي لا يمكن فيها قول كل شيئ، وانطلاقا من كلامنا يمكن أن تمارس علينا الرقابة أو المراقبة ومن ثمة التعرض إلى عواقب غالبا ما تقوم على مزايدات مختلفة الاتجاهات والأهداف. يتعرض الحق في حرمة الحياة الخاصة أيضا إلى انتهاكات وذلك لأنه لا وجود للتستر من وجهة نظر قانونية ويمارس فقط بفضل حلول تقنية. أصبح احترام الخصوصية حقا مصطنعا للغاية لأنه من خلال تقنيات المراقبة والتعقب، أصبحت تصرفاتنا مراقبة بشكل دائم، حتى ولو كانت الطرق التعرف على الأشخاص هي أبعد ما تكون عن الكمال. تتم هذه المراقبة في جزء كبير من خلال مراقبة تدفق البيانات، ولكن لم يعد من الممكن فصل أعمالنا في الفضاء الرقمي عن تلك الممارسة في العالم المادي طالما أن أنظمة المراقبة بالفيديو[1] أو البيومترية تدرك تحقق وجود صلة بين هذين العالمين.

ويضاف إلى ذلك ملاحظة تتمثل في أن توفير الأدوات المتاحة للاتصال إلكترونيا يترك للمبادرة الخاصة لمقدمي الخدمات على الإنترنت. يبدو أن المشرع قد تنصل من مهمته المتمثلة في حماية الأفراد، وذلك باختيار الدفاع عن النظام العام بدلا من الدفاع عن الحريات الأساسية الفردية والجماعية. من خلال النصوص المليئة بالالتزامات والممنوعات، حيث تعتبر السلطات العمومية مستخدم الإنترنت كمستهلك أو كمجرم محتمل، ولكن نادرا جدا ما تعتبره كفرد، وجزء من مجتمع يجب حماية ممتلكاته المشتركة.

إن احترام الحريات العامة لا يتناقض مع حتمية الأمن. بل على العكس من ذلك فإن حمايتها تشكل حراسة لديمقراطياتنا. فلا يمكن فصل الحرية عن الأمن،

---

[1] وحسب المرسوم الرئاسى رقم 15 – 228 المؤرخ فى 22 أوت 2015 يعتبر النظام الوطنى للمراقبة بواسطة الفيديو، وسيلة تقنية للاطلاع و الاستباق، يهدف إلى المساهمة في مكافحة الإرهاب والوقاية من الأعمال الإجرامية وحماية الأشخاص والممتلكات والحفاظ على النظام العام وكذا ضبط حركة السير عبر الطرق و معاينة المخالفات وتأمين البنايات والمواقع الحساسة وتسيير وضعيات الأزمة أو الكوارث الطبيعية أو غيرها.

ويتوقف توازنهما على الضمانات وأساليب الرقابة التي تتعلق بها. كم عدد المرات التي قيل فيها أن الحرية الحقيقية هي الأمن؟ أو أن الأمن الأول هو الحرية؟ في الحقيقة فإن الأمن جزء لا يتجزأ من الحريات العامة للأفراد – مثل حرية التعبير أو الحق في حرمة الحياة الخاصة. ولا ينبغي وضعه على الجانب الآخر من الميزان، بل يقترن بحريات أخرى في نظام تكاملي. إن الوصفة تكمن في المحافظة على النسب الصحيحة بين الحقوق المختلفة: إن النظام الكل أمني يشكل تهديدا لحرية التعبير وحرمة الحياة الخاصة. ومن شأن نظام غير آمن بدرجة كافية ألا يفي بالحاجة الاجتماعية إلى توفير السلم. وفي بعض الحالات يسمح الترابط بين الحرية والأمن بتعزيز بعضها البعض. إن الحرية القصوى في جميع مجالات الحياة في المجتمع يجب أن تكون دائما المبدأ، نقطة البداية التي يجب أن تكون بها جميع تدخلات الدول والمتعاملين الخواص في مجال الأمن محدودة ومبررة وشفافة. إن الاحتفاظ بالبيانات والوصول إليها واستخدامها من طرف السلطات الوطنية المختصة ومقدمي الخدمات يجب أن يقتصر على ما هو ضروري ومتناسب في مجتمع ديمقراطي. ويجب أن يخضع لضمانات أساسية وفعّالة حتى لا يؤدي إلى إنشاء مجتمع بوليسي الكل فيه مشتبه فيه.

مثل أي عمل أمني فإن مكافحة الجرائم المرتكبة على الانترنت عملية تبقى معقدة.

ويجب أن تهدف إلى حماية الأشخاص والسلع المادية وغير المادية والدفاع عن قيم المجتمعات الديمقراطية[1]. وفي هذا السياق فإنه وحدها مقاربة متعددة التخصصات ومتكاملة إزاء ظاهرة الجريمة الالكترونية ومكافحة الإرهاب

[1] Solange Ghernaouti-Hélié, Arnaud Dufour, « Cybercriminalité et cybersécurité », dans « Internet », Que sais-je, PUF, 11ème éd., 2012, p. 94-108.

الإلكتروني تتيح اتخاذ التدابير الوقائية والتفاعلية المناسبة التي تعتمد فعاليتها على اكتمالها وجدواها التقنية واتساقها على الصعيدين الوطني والدولي. والغرض من أي شكل من أشكال التدخل التشريعي يجب أن يتمثل في حتمية ضمان مستوى مقبول من التوفيق بين الحريات مع تجديد أساليب التنظيم المعمول بها. ويتمثل التحدي في الانتقال من المبادرات الفردية وغير المتزنة إلى تنظيم كامل ومتناسق للوجود الرقمي.

قائمة المراجع

أولا: المـــراجع باللغة العـــربية.

✓ **الكتـــــب:**

1. أحسن بوسقيعة، المنازعات الجمركية، دار هومة، الطبعة الثانية، الجزائر، 2005.

2. حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة ، دراسة مقارنة، دار النهضة العربية،.1978.

3. عبد الرؤوف مهدي، حدود حرية القاضي في تكوين عقيدته، مؤسسة العين للطباعة، دون دار للنشر، دون سنة الطبع.

4. عبد الغاني بسيوني عبد الله، النظم السياسية، أسس التنظيم السياسي ــ الدولة ــ الحكومة ــ الحقوق و الحريات العامة، الدار الجامعية، بيروت لبنان، 1984.

5. عبد المنعم محفوظ – علاقة الفرد بسلطة الحريات العامة وضمانات ممارستها – المجلد الاول والثاني ط2 – دار الهناء للطباعة – القاهرة، 1989.

6. محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة، ط1، منشورات دار النهضة العربية، القاهرة، 1993

7. مروة زين العابدين صالح، الحماية القانونية الدولية بين القانون الدولي الاتفاقي والقانون الوطني، ط1، مركز الدراسات العربية للنشر و التوزيع، 2016.

8. أسامة سمير حسين، الاحتيال الالكتروني، الأسباب والحلول، ط1، عمان، الجنادرية للنشر والتوزيع، 2011.

9. أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية، القاهرة– مصر، 1994

10. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994.

11. أمحمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد في الجزائر العاصمة يوم 29 مارس 2017.

12. بهاء شاهين، شبكة الانترنت، العربية لعلوم الحاسب، القاهرة– مصر، 1996.

13. بولين انطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية ، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2009.

14. جاك لاريو، قانون الانترنت، المنظمة العربية للتنمية الإدارية، ترجمة محمد سيد توفيق، الطبعة الاولي، القاهرة، 2009.

15. جبران خليل جبران، رمل وزبد، ترجمة ثروت عكاشة الطبعة السادسة، دار الشروق، القاهرة– مصر، 1999.

16. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة. 2001.

17. جوليا أنغوين، سلطة شبكات التعقب عبر وسائل الاتصال و الأنترنت، ترجمة حسان البستاني، الدار العربية للعلوم ناشرون، ط1، بيروت، 2015.

18. حسني المصري، الكمبيوتر كوسيلة فنية لإنسياب المعلومات عبر الحدود الدولية وصور إستغلاله التجاري الدولي. ممؤسسة الكويت للتقدم العلمي، ط1، 1994.

19. الحمادي حسن، عقود و خدمات المعلومات، دراسة في القانون المصري والفرنسي، دار الثقافة للنشر و التوزيع، عمان، الأردن، الطبعة الأولى، 2003.

20. سعيد عبد اللطيف، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية،مصر، 1999.
21. شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، دار الفكر و القانون، ط1، المنصورة، 2015.
22. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، ط1، الاسكندرية، 2009.
23. عبد الكريم العيلي، الحريات العامة في الفكر و النظم السياسية في الاسلام – دراسة مقارنة – القاهرة، دار الفكر العربي، 1983.
24. عصام عبد الفتاح مطر، الحكومة الالكترونية بين النظرية و التطبيق، دار الجامعة الجديدة، ط1، الاسكندرية، 2013.
25. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، جامعة باتنة1 الجزائر. كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 2425|03|2017.
26. محمد عبد المحسن المقالع، حماية الحياة الخاصة للأفراد وضمانتها في مواجهة الحاسوب الآلي، الكويت، 1992.
27. محمد فتحي، تفتيش شبكة الأنترنت لظبط جرائم الاعتداء على الآداب العامة، المركز القومي للاصدارات القانونية، ط1، الاسكندرية، 2012.
28. محمد لعقاب، المواطن الرقمي، دار هومة، ط2، الجزائر، 2013.
29. محمد محمد الألفي، المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت، 2005.
30. محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة، ط1، منشورات دار النهضة العربية، القاهرة.
31. مدحت رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية، 2001.

32. مصطفى يوسف كافي، التجارة الإلكترونية، دار رسلان للطباعة والنشر والتوزيع، الطبعة الاولي، دمشق، 2009.
33. نعيم مغبغب، مخاطر المعلوماتية والانترنت دار النهضة العربية القاهرة – 1998.
34. هدى حامد قشقوش، جرائم الحاسب الالكترونى فى التشريع المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992.
35. هشام ملاطي، خصوصية القواعد الإجرائية للجرائم المعلوماتية محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع،2014
36. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة – ط1 – دار النهضة العربية، 2008.

✓ **أطروحات الدكتوراه:**

37. محمد عبد العظيم محمد، حرمة الحياة الخاصة في ظل التطور العلمي الحديث، رسالة دكتوراه، جامعة القاهرة، كليّة الحقوق، 1988.
38. صفية بشاتن، الحماية القانونية للحياة الخاصة دراسة مقارنة، رسالة دكتوراه، جامعة تيزي وزو، كليّة الحقوق، 2012.
39. محمد عبد العظيم محمد، حرمة الحياة الخاصة في ظل التطور العلمي الحديث، رسالة دكتوراه، جامعة القاهرة، كليّة الحقوق، 1988.

✓ **المجلات والمقالات:**

40. جبار فطيمة، مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، العدد الثالث ديسمبر 2016.

41. عبد العال الديربي، الجريمة المعلوماتية – تعريفها – أسبابها وخصائصها، 13 يناير 2013.

42. محمودي نور الهدى، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد 11، جوان 2017.

✓ **القوانين والمراسيم:**

1- القوانين:

43. القانون رقم 16-01 مؤرخ في 26 جمادى الاولى عام 1437 الموافق ل 6 مارس. سنة 2016 يتضمن التعديل الدستوري.

44. القانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

45. القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

46. القانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل و يتمم الأمر رقم 66-155المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966. و المتضمن قانون الإجراءات الجزائية.

47. الأمر رقم 15-02 المؤرخ في 23 جويلية 2015 المعدل و المتمم. للأمر رقم 66-155 المؤرخ في 8 جوان 1966 والمتضمن قانون الإجراءات الجزائية.

48. القانون رقم 14/03 الصادر في 24 فيفري 2014 المتعلق بسندات وثائق السفر.

2- المراسيم والقرارات:

49. المرسوم الرئاسي رقم 261-15 مؤرّخ في 8 أكتوبر سنة 2015 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
50. المرسوم الرئاسي رقم 15 - 228 المؤرخ في 22 أوت 2015 و الذي يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو.
51. مرسوم رئاسي رقم 17-143 مؤرخ في 21 رجب عام 1438 هجري الموافق 18 أبريل سنة 2017 يحدد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها وتجديدها
52. قرار مؤرّخ في 9 ذي القعدة عام 1431 الموافق 17 أكتوبر سنة 2010، يحدّد المواصفات التقنية لمستخرج عقد ا لميلاد الخاص باستصدار بطاقة التعريف الوطنية وجواز السفر.
53. قرار مؤرّخ في أوّل صفر عام 1433 الموافق 26 ديسمبر سنة 2011، يحدد المواصفات التقنية لجواز السفر الوطني البيومتري الإلكتروني.
54. قرار مؤرّخ في أوّل صفر عام 1433 ا لموافق 26 ديسمبر سنة2011، يحدد تاريخ بداية تداول جواز السفر الوطني البيومتري الإلكتروني.
55. قرار مؤرخ في 22 جمادى الثانية عام 1432 الموافق 25 مايو سنة 2011 يتعلق بملف طلب بطاقة التعريف الوطنية و جواز السفر.

ثانيا: المـــراجــــــع باللغة الأجنبـــــية.

✓ **الكتـــــب:**

1. *Agathe LEPAGE: Libertés et droits fondamentaux à l'épreuve de l'internet, Litec, 2002.*

2. *Ahmed Dahmani, José Do-Nascimento, Jean-Michel Ledjou, Jean-Jacques Gabas, « La Démocratie à l'épreuve de la société numérique », éd. Karthala, Paris 2007.*

3. *Ahmed MAHIOU: Cours de contentieux administratif, OPU, 1981.*

4. *Antoinette Rouvroy, « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? », in Stéphanie Lacour (dir.), La sécurité de l'individu numérisé. Réflexions prospectives et internationales, Paris, L'Harmattan, 2009.*

5. *Bernard Beignier, « L'honneur et le droit », LGDJ 1995.*

6. *Bernard Beignier, « Le droit de la personnalité », PUF, Que saisje ?, 1992.*

7. *Béatrice Vacher, « Communication et débat public: les réseaux numériques au service de la démocratie », Paris, l'Harmattan, 2013 .*

8. *Bensoussan Alain , Internet, aspects juridiques, Paris, Hermes, 1996.*

9. *Bensoussan Alain, Salvator Maurice, Risques informatiques, parades et techniques juridiques, París, Editions des Parques, 1983.*

10. *Claude Jean Devirieux, « Manifeste pour le droit à l'information, de la manipulation à la législation », Presse de l'Université du Québec, Québec, 2009.*

11. *Claudine Guerrier, MarieChristine Monget, Droit et sécurité des télécommunications. Edition Springuer, 2000.*

12. *Claudine Guerrier, MarieChristine Monget, Droit et sécurité des*

télécommunications. Edition Springuer, 2000.

13. *Claudine Guerrier, MarieChristine Monget, Droit et sécurité des*

télécommunications. Edition Springuer, 2000.

14. *COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 29 Rapport d'activité, Paris, La Documentation française, Paris, 2009.*

15. *Conseil d'Etat, Étude annuelle 2014: Le numérique et les droits fondamentaux, la documentation française.*

16. *Duaso-Calès*, *Rosario*,

Principe de *finalité*, *protection* des données et *secteur public*: la

gouvernance des *structures* en *réseau*, Thèse de doctorat, 14 octobre *2011*, Universités CRDP-*Montréal*-Paris II.

17. *Eric Sadin, Surveillance globale. Enquête sur les nouvelles formes de contrôle , Paris, Climats, 2009.*

18. *Frédéric Sudre, « Droit européen et international des droits de l'homme », PUF, coll. « Droit fondamental », 7e éd.*

19. *François Rigaux, « La protection de la vie des autres biens de la personnalité », Bruylant-LGDJ, 1990.*

20. *Frédéric Jérôme Pansier: La criminalité sur internet, éd. Puf, 2000.*

21. *FrédéricJérôme Pansier: La criminalité sur internet, éd. Puf, 2000.*

22. *Gerard Cornu, « Vocabulaire juridique », 8ème éd .*

23. *Eric Freyssinet, Guillaume Desgens-Pasanau, « L'identité à l'ère numérique », DallozSirey, Coll. Presaje, 2009.*

24. *GARRAM Ibtissem, Terminologie juridique dans la législation algérienne, lexique Français, Arabe, ENAG, Alger, 1992.*

25. *Georges BURDEAU: Les libertés publiques, 4ème édition, L.G.D.J, 1972.*

26. *Henrii Oberdorff, « Droits de l'Homme et libertés fondamentales », 2ème éd., LGDJ, n° 395.*

27. *Jacques Robert, Jean Duffar Droits de l'homme et libertés fondamentales, Montchrestien, 1999.*

28. *Jean et Frayssinet Jean, Les libertés individuelles à l'épreuve des Ntic, Pul, 2001.*

29. *Jean Louis COSTA: Liberté, ordre public et justice en France, Tome 1, Paris, 1965.*

30. *Jean MORANGE: "Libertés publiques", Collection Que saisje, N° 26708, PUF, Paris.*

31. *Jean Pierre Chamoux: Menaces sur lordinateur, éd. Seuil, 1986.*

32. *Jean RIVERO: Les libertés publiques, Tome 1, Les droit de l'homme, PUF, 2003.*

33. Jean et Frayssinet Jean, Les libertés individuelles à l'épreuve des Ntic, Pul, 2001.

34. JeanPaul Costa, les libertés publiques en France et dans le monde STH, Paris, 1986.

35. Jean-Marie Auby, Robert Ducos-Ader, « Droit de l'information », D., 1982.

36. Limore Yagil, « Internet et les droits de la personne, nouveaux enjeux éthiques à l'âge de la mondialisation », Les éditions du CERF, Paris, 2006.

37. Lexique des termes juridiques, 19ème éd., Dalloz 2012 .

38. Lilian edwards and charlotte waeldelaw and the internet, "Rugulating cyber space", hart publishing,exford.1997.

39. Gilles Goubeaux, « Les personnes, Traité de droit civil, Les personnes », LGDJ, n° 280 et s.

40. Myriam Quéméner, Criminalité économique et financière à l'ère numérique, Economica 2015.

41. Marie-Anne Frison-Roche, Internet espace d'interrégulation, dalloz, Mai 2016.

42. Marie-Christine Piatti: Les libertés individuelles à l'épreuve des NTIC, PUL, 2002.

43. Mireille Delmas-Marty. Criminalité économique et atteintes à la dignité de la personne. Éditions de la Maison des sciences de l'homme, Paris, 1997.

44. Norbert Wiener, « Cybernétique et Société. L'usage humain des êtres humains », Paris, Union générale d'éditions, 1971.

45. Nidal El Chaer: La criminalité informatique devant la justice pénale, edition Sader, 2004.

46. Olivier Itéanu, « L'identité numérique en question », Paris, Eyrolles, 2008.

47. *Philipe BRAND: La notion de liberté publique, LGDJ, Paris, 1968.*

48. *Philippe Rose: La criminalité informatique à l'horizon 2005 Analyse prospective, editions L'Harmattan, 1992.*

49. *Pierre DEPREZ et Vincent FAUCHOUX. Lois, Contrats et Usages du. Multimédia, ed. Dixit, 1997.*

50. *Pierre KAYSER, La protection de la vie privée par le droit, Economica / Presses universitaires d'AixMarseille, 3° éd., 1995*

51. *Raymond Saleilles, « Essai d'une théorie de l'obligation d'après le projet de code civil allemand », Hachette Livre BNF. 2012 ;*

52. *Robert Charvin et JeanJacques Sueur: Droits de l'homme et libertés de la personne, 2eme edition, Litec, 1997.*

53. *Solange Ghernaouti-Hélié, Arnaud Dufour, « Cybercriminalité et cybersécurité », dans « Internet », Que sais-je, PUF, 11ème éd., 2012.*

54. *Steven Levy, « L'Ethique des hackers », Paris, Globe, 2013.*

55. *Tim BernersLee, « Long Live the Web », Scientific American (2010) 303, n° 6.*

56. *Toby Mendel, « Liberté de l'information, étude juridique comparative », 2008, 2ème éd.*

✓ **المجلات والمقالات باللغة الأجنبية:**

57. *Antoine LATREILLE: La protection juridique des bases de données électroniques, Revue Internationale du Droit d'Auteur, n°164, avril 1995.*

58. *Antoine LATREILLE: La protection juridique des bases de données électroniques, Revue Internationale du Droit d'Auteur, n°164, avril 1995.*

59. *Cédric Michalski, La recherche et la saisie des preuves électroniques,*

Gazette du Palais - 11/02/2014 - n° 042.

60. *Chantal Enguehard, « Internet. Avec Obama, bienvenue à la Maison*
Blanche 2.0 », Jus Politicum, Revue de droit politique et de droit
constitutionnel, n° 2, janv. 2009.
61. *Christine Causse Gabarrou, « Les transferts de données à caractère*
personnel dans la proposition de Règlement du Parlement européen et
du Conseil et compétitivité des entreprises: perspectives d'amélioration
», RLDI, 2013, n° 98.
62. *David El Sayegh, « Le Conseil constitutionnel et la loi Création et Internet: une décision en trompel'oeil », Lég., n° 263, 2009.*
63. *Emmanuel Derieux, « Lutte antiterrorisme et protection des données*
personnelles: Durée de conservation des données de communication
Invalidité de la dir. n° 2006/24/CE », RLDI 2014, n° 104, mai 2014.
64. *Dominique Wolton, l'espace public, cahiers français, N° 218, Mai Juin*
1997.
65. *Eric A. Caprioli, « Les flux transfrontières des données à caractère*
personnel en matière bancaire », RDBI., 2010, n°1.
66. *Emilie Bailly, « L'entreprise face aux risques informatiques: les réponses du droit pénal », RLDA 2011, n° 64.*
67. *Etienne Montero et Quentin Van Enis, « Ménager la liberté d'expression au regard des mesures de filtrage imposées aux intermédiaires de l'Internet: La quadrature du cercle ? », RLDI, mai 2010, n°60.*

68. *Eléonore Varet, « L'Open Data. Point de rencontre entre le libre et les données publiques », Expertises, n° 371, juill. 2012.*

69. *Emmanuel DERIEUX: Internet et protection des données personnelles, Revue Lamy Droit de l'Immatériel, 2008.*

70. *Emmanuel Pierrat, « Protection des droits de la personnalité »,*

Legicom, n° 2, 1996.

71. *Emmanuel VALJAVEC, « Internet, un nouvel espace de liberté sous surveillance », Études 2013/3(Tome 418).*

72. *Florence Chaltiel, « La loi Hadopi devant le Conseil constitutionnel » LPA, n° 125, 24 juin 2009.*

73. *Georges Kellens: Revue internationale de criminologie et de police technique, 1991, n.2.*

74. *Hervé Croze, « L'apport du droit pénal à la théorie générale du droit de l'informatique», JCP 1988. I. 3333.*

75. *Hackers: Heroes of the Computer Revolution. Front Cover. Steven Levy. Anchor Press/Doubleday, 1984 Computer hackers.*

76. *Isabelle FalquePierrotin, la constitution et l'internet, Dalloz « Les Nouveaux Cahiers du Conseil constitutionnel », 2012/3 N° 36.*

77. *Julien Levrel, « Wikipedia, un dispositif médiatique de publics*

participants »,

78. *Jennifer Marchand, « L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique », JCP A, n° 7, févr. 2014.*

79. *Jeoffrey Sabbah, « L'appréhension de l'identité sur Internet », RLDI, n° 101, févr. 2014.*

80. *J.P. Gridel, A. Lacabarats, « Droit à la vie privée et liberté d'expression: fond du droit et action en justice », Gaz. Pal 17/19 nov. 2002, n°321 à 323, Doct.*

81. *Jean-Claude BONICHOT, La cour de justice de l'Union européene et les nouvelles technologies de l'information: vers une cour 2.0 ? Petites affiches 15/03/2016 n° 53.*

82. *Jean-Michel Bruguière, « Loi « sur la protection de la création sur Internet »: mais à quoi joue le Conseil constitutionnel ? », D. n° 26, 2009.*

83. *Jean-Pierre Ancel, « Protection de la personne: image et vie privée », Gaz. Pal., 26 sept. 1994.*

84. *Jean-Philippe Feldman, « Le Conseil constitutionnel, la loi « Hadopi » et la présomption d'innocence », JCP G, n° 28, 2009.*

85. *Laurent Cohen-Tangui, « Le clair obscur d'internet: Transparence et secret », Pouvoirs, n° 97, 2001.*

86. *Laure Marino, « Le Droit d'Accès à Internet, Nouveau Droit Fondamental », D., n° 30, 2009, n° 2045.*

87. *Laure Maude, « Les nouveaux territoires des droits de la personnalité », Gaz. Pal., 1819 mai 2007.*

88. *Laurence Tellier*-Loniewski, Anne *PLATON*, Alain *Bensoussan* « Loi « création et Internet »: le feuilleton législatif continue... suite et fin ? », Gaz. Pal., n° 203204, 22 et 23 juill. 2009.

89. *Louise Cadoux: Les reponses technologiques. LPA, 10/11/1999, n.224.*

90. *Marc Domingo, « Protection de la vie privée et liberté des médias », Gaz. Pal., 3031 déc. 1994.*

91. *Michel Verpeaux, « La liberté de communication avant tout. La censure de la loi Hadopi 1 par le Conseil constitutionnel », JCP G, n° 39, 2009.*

92. *Marie-charlotte Roques-Bonnet, Le droit peutil ignorer la révolution numérique ?, Michalon, 2010, p. 332 ; N. Sautereau, « Internet et le droit global: approche critique », L'observateur des Nations unies, 20112, vol. 31.*

93. *MAISL HERBERT, Communications mobiles, secret des correspondances et protection des données personnelles, LPA, 21 juin 1995, n.74.*

94. Louise MERZEAU, Michel ARNAUD*, « Traçabilité et réseaux », Hermès, n° 53, avr. 2009*

95. *MEILLAN, Eric: Les menaces à la sécurité des systèmes d'information.: la réponse des institutions françaises,*

Revue Internationale de Police Criminelle, Lyon, V.430 (MaiJuin 1991).

96. *MEILLAN, Eric: Les menaces à la sécurité des systèmes d'information.: la réponse des institutions françaises, Revue Internationale de Police Criminelle, Lyon, V.430 (MaiJuin 1991(*

97. *MERZEAU Louise, « De la surveillance à la veille », Cités, vol. 3, n° 39,2009.*

98. *Michel Verpeaux, La loi sur le renseignement, entre sécurité et libertés, la semaine juridique édition générale n° 38 14 septembre 2015.*

99. *Myriam QUÉMÉNER, Les données personnelles à l'ère numérique Quelle protection sur le plan pénal ? Revue du droit public 01/01/2016 n° 1.*

100. *Myriam Quéméner, Les spécificités juridiques de la preuve numérique, AJ Pénal 2014.*

101. *Olivier Violeau, Les techniques d'investigations numériques: entre insécurité juridique et limites pratiques, AJ Pénal, 2017, p.324*

102. Philippe *Mouron, « Internet et identité virtuelle des personnes », RRJ 2008, n° 124.*

103. *Patrice Spinosi, « Le secret d'affaires et le secret du patrimoine. Face aux droits et libertés individuels », DP, n° 233, févr 2014.*

104. *Pierre-François Docquir, « Le « droit de réponse 2.0 » ou la tentation d'un droit subjectif d'accès à la tribune médiatique »,Revue de Droit de l'U.L.B., n° 35, 2007.*

105. *Rosa Chun, Gary Davies, « E-reputation: the role of mission and vision statement in positionning strategy », Journal of Brand Management, Vol. 8, n°. 4 et 5, mai 2001.*

106. *Romain Gola, « Usurpation de l'identité sur l'Internet: aspects de droit pénal comparé », RLDI 2009/55, n° 1839.*

107. *Ronan Le Roux, « L'homéostasie sociale selon Norbert Wiener », Revue d'histoire des sciences humaines, n° 16, 2007.*

108. *Roger A. Nowadzky, « A Comparative Analysis of Public Records Statutes », 28 The Urban Lawyer, 65 (1996). JP., Chamoux, « Données publiques », Les Cahiers du numérique 1/ 2013, vol. 9.*

109. *Rapport d'information, Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, 2015.*

110. *Robert Badinter: Le droit au respect de la vie privée", JCP 1968, n.2136.*

111. *Robert Lindon, La presse et la vie privée, J.C.P 1965, 1, 1987.*

112. *Sarra Soltani, « Big Data et le principe de finalité », RLDI, n° 97, oct.*
2013.

113. *Sophie Coignard. internet. Le reseau qui fait peur aux services secrets. Le Point, 29 juillet 1995, n.123.*

114. *Thierry Vedel, « Les politiques des autoroutes de l'information dans les pays industrialisés: une analyse comparative », Réseaux, 1996, n° 78.*

115. *Wanda Mastor, La loi sur le renseignement du 24 juillet 2015 « La France, Etat de surveillance » ? AJDA 2015.*

116. *Yves POULLET: Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information, Droit de l'Informatique, 1987, n.4.*

117. *Georges Kellens: Revue internationale de criminologie et de police technique, 1991, n.2.*

118. *Yves POULLET: Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information, Droit de l'Informatique, 1987, n.4.*

قائمة المحتويات